Cyberterrorisme

- Fakta eller fiksjon?

Tonje Grunnan

Hovedoppgave i statsvitenskap

Universitetet i Oslo

Institutt for statsvitenskap

Våren 2007

Forord

Ideen til å skrive en hovedfagsoppgave om cyberterrorisme kom i forbindelse med en sommerjobb jeg hadde på prosjektet TERRA (Terrorisme og asymmetrisk krigføring) ved Forsvarets forskningsinstitutt (FFI). Min oppgave var blant annet å drive informasjonssøk rundt begrepet cyberterrorisme og andre beslektede begreper for å prøve å komme nærmere en idé om hva dette begrepet innebar, om det var gjennomført noen cyberterroristangrep, og om det var en reel trussel for å bli utsatt for dette. Denne informasjonsinnhentingen ga meg inspirasjon til å skrive min hovedoppgave i statsvitenskap om nettopp cyberterrorisme. Det ville være interessant og nyskapende å koble dette nye begrepet til statsvitenskapelig teori og metode. Jeg fikk etter hvert studieplass ved FFI og hadde stort utbytte og lærte mye av å sitte sammen med instituttets terrorismeforskere og andre forskere. Jeg vil rette en stor takk til FFI for at jeg fikk muligheten til jobbe med oppgaven i et skapende og vitenskapelig miljø. Det viste seg imidlertig å være en stor utfordring å skrive denne oppgaven ettersom noe lignende ikke var gjort før, og jeg er derfor svært fornøyd med at prosjektet nå er gjennomført. Jeg vil spesielt takke veileder og forsker Anders Kjølberg ved FFI som har gitt meg konstruktive tilbakemeldinger i alle de ulike fasene av arbeidet og vært til stor hjelp. Tusen takk til Ragnhild Vingsand for utlån av ”skrivestue” og god musikk til arbeidet! Jeg vil også rette en stor takk til Ina E. Bøe som leste gjennom deler av sisteutkastet i innspurten og ga meg nyttige kommentarer. Og ikke minst, tusen takk til Trond, familien og alle mine venner som har oppmuntret meg og inspirert meg til å bli ferdig.

Skjetten, 22.april 2007

Tonje Grunnan

Innhold

1. Innledning

”Tomorrow’s terrorists may be able to do more with a keyboard than with a bomb.”[1]

Formålet med oppgaven er å studere informasjonsrevolusjonens påvirkning på sikkerhetspolitikken, og da spesielt hvilken betydning den har hatt for terrorismens ”utvikling” og særlig framveksten av begrepet *cyberterrorisme*. Den nye æra, Informasjonsalderen, skapte store forandringer mot slutten av 1900-tallet. Verden er blitt mer nettverksbasert, vitale informasjonssystemer er forbundet med hverandre, vi er blitt avhengige av informasjonsteknologi (IT), og i takt med denne utviklingen har de moderne samfunn blitt mer sårbare. Vi har fått et nytt sosioøkonomisk system preget av informasjonsteknologi, nettverksbygging og globalisering (Castells 1999:2). I de senere år har nye begreper som cyberterrorisme, cyberkrig, nettkrig og informasjonskrigføring fått stor oppmerksomhet i media, men også blant forskere, politikere og spesialister innen informasjonssikkerhet. Man ser for seg dramatiske scenarier hvor terrorister eller fremmede makter bruker informasjonsteknologi som våpen for å forstyrre instrumentene i fly slik at de styrter, forårsake alvorlige strømbrudd som kan sette et stort samfunn ut av spill og lignende. Man frykter at ulike aktører eller enkeltpersoner vil kunne bruke nye midler som å hacke seg inn på en stats operative datasystemer for å ødelegge telekommunikasjonssystemet framfor å bruke de tradisjonelle bombene.

Det finnes ikke én allment akseptert definisjon av begrepene cyberterrorisme og informasjonskrigføring, og mye av det som skrives om disse trendene er vagt og uklart fordi det er nye fenomener som man fortsatt ikke vet nok om. Er det mulig å gi en klar definisjon av begrepene, og kan de brukes om hverandre eller er de for forskjellige?

---

[1] *Compters at Risk*, National Academy Press, 1991 (sitert i Denning 1999:70).

Ved bruk av såkalte nye cybervåpen eller informasjonskrigføringsvåpen er det i større grad enn før mulig å omgå militære institusjoner og infiltrere militær og sivil infrastruktur, noe som kan gjøre en motpart stor skade. Slike trusler har ført til bevisstgjøring om samfunnets sårbarhet, og flere stater har opprettet forskningsprogram som skal utarbeide løsninger som kan forbedre sikre landet mot fiendtlige stater og cyberterrorister. Diverse tester og spill, som f.eks. dataangrep mot egne systemer[2], har blitt gjennomført for å avdekke sårbarheter, farer og trusler ved et cyberangrep på deler av infrastrukturen.

I tiden rundt milenniumskiftet begynte begrepet cyberterrorisme å versere i det akademiske miljø. Begrepet oppstod på 1980-tallet, men ble for alvor brukt i forbindelse med år 2000-problematikken da man fryktet hva som kunne skje i vårt teknologiavhengige samfunn. Det ble også skrevet mye om den nye cybertrusselen, spesielt i amerikanske tidsskrifter og presse. Politikere, som for eksempel Bill Clinton, begynte også å interessere seg for cyberterrorisme og beskyttelse av kritisk infrastruktur (se White Paper 1998) allerede før år 2000, men også etterpå, noe Bush-administrasjonen også har vært opptatt av.

Terrorangrepene i New York 11.september 2001 var ikke cyberterrorisme, men en terrorhendelse som viste at terrorister har evnen til å overraske med utradisjonelle midler. I disse angrepene var de kaprede flyene våpnene (midlene), og man kan tenke seg at terrorister også kan være i stand til å benytte seg av cybervåpen ved en senere anledning. Internett er allerede en etablert arena for propaganda og psykologisk krigføring, et sted hvor man kan planlegge handlinger (Alexander og Swetnam 2001). O'Day (2004:xi) skriver følgende om cyberterrorisme: "It is the convergence of terrorism and cyberspace, bringing together two significant modern fears: the fear of technology and the fear of terrorism". Samfunnets sårbarhet har økt som følge av globaliseringen og informasjons- og teknologiavhengighet. Cyberspace er en ny potensiell arena for terroraksjoner og krigføring, og terrorister kan potensielt bruke

[2]Se bl.a. http://www.csis.org/pubs/cyberter.html

informasjonsvåpen, såkalte cybervåpen, i kampen for å fremme sine interesser og utnytte denne sårbarheten. Spørsmålet er om det er sannsynlig at vi vil bli utsatt for cyberterrorisme slik det blir hevdet i mange bøker og artikler.

1.1 Problemstilling

Det er mange aviser og tidsskrifter som skriver om og rapporterer såkalte cyberangrep, og det finnes både seriøse og useriøse organisasjoner som har sider på Internett som omtaler cyberterrorisme. Med andre ord, økt oppmerksomhet er rettet mot cyberterrorisme og relaterte begreper, og hvis man leser rapporter, artikler, Internettsider og lignende om emnet, kan man ved første gangs lesning føle at trusselen er meget stor. Leser man med et mer kritisk blikk derimot, kan det synes som om trusselen er noe overdramatisert. Det er frykt for cyberangrep og det settes inn ressurser[3] på å kartlegge og eventuelt forhindre denne nye trusselen.

Samtidig er det et paradoks at det hittil ikke er rapportert om cyberangrep av alvorlig art som har truet nasjonal sikkerhet og skadet mennesker. Derfor kan det kanskje stilles spørsmål ved berettigelsen av all denne oppmerksomheten. Det finnes mange empiriske eksempler på såkalte cyberangrep, men poenget er at selv den minste hackingepisode kan slås opp som en meget alvorlig hendelse. Hvor går grensen på hva som er cyberterrorisme, cyberangrep og hva som er en hacking-insident? Er trusselen for cyberterrorisme overdrevet?

Jeg ønsker på bakgrunn av dette å etablere cyberterrorisme som en del av *sikkerhetspolitikken* og måten jeg vil gjøre det på er å studere diskursen rundt begrepet cyberterrorisme. Jeg har ikke funnet litteratur hvor cyberterrorismebegrepet er satt inn i en statsvitenskapelig kontekst med en teoretisk forankring, og det vil

[3] I USA satte for eksempel president Bill Clinton i gang prosjekter som skulle utrede farene ved og eventuelt mottiltak mot cyberangrep, og diverse institusjoner som Terrorism Research Center og Infowar Center har blitt opprettet i USA. Dette kommer jeg tilbake til i analysekapitlene.

denne oppgaven gjøre for å gi begrepet cyberterrorisme en ny vinkling.

Jeg vil forsøke å knytte framveksten av begrepet cyberterrorisme til endringen av sikkerhetsbildet etter den kalde krigen – en tid hvor en ny sikkerhetsagenda har blitt skapt. En tid hvor også verden har blitt mer global og teknologiutviklingen har skapt sårbare samfunn avhengige av kritiske infrastrukturer. Oppgaven skal søke å gi svar på følgende problemstilling:

Kan cyberterrorisme sies å ha blitt sikkerhetisert og dermed satt på den sikkerhetspolitiske agenda?

Oppgaven vil ta form av en diskursanalyse der jeg kartlegger det som skrives på området av ulike aktører og drøfter og kommenterer diskursen rundt begrepet. Jeg vil fokusere på selve diskursen til de ulike gruppene som fremmer cyberterrorisme som en fare og analysere hvordan begrepet fremstilles og brukes. Hovedpoenget er ikke selv å skulle vurdere trusselen for da kan jeg lett bli en del av den diskursen jeg vil analysere. For å kunne svare på problemstillingen må jeg forsøke å klargjøre hva cyberterrorisme er og samle trådene i diskursen som finnes på dette feltet. I tillegg vil jeg knytte begrepet til et teoretisk rammeverk som kan bidra til å belyse om cyberterrorisme er i ferd med å oppfattes som en del av sikkerhetspolitikken.

1.2 Valg av teori og metode

1.2.1 Teori

Oppgaven tar utgangspunkt i én teoretisk tilnærming til sikkerhet, den såkalte Københavnerskolens sikkerhetspolitiske rammeverk. Københavnerskolens rammeverk går ut på å holde sikkerhetsagendaen åpen for mange ulike typer trusler, disse truslene utforskes i forhold til referanseobjekter, og sikkerhetiseringen

(”securitization”)[4] av trusselen kan være ikke-militær så vel som militær (Buzan 1997:13). I denne konteksten vil det være interessant å studere cyberterrorisme. Oppfatninger og syn på trusler og sikkerhet har endret seg etter den kalde krigens slutt. Den internasjonale politiske struktur er ikke lenger bipolar, preget av supermaktsrivaliseringen mellom USA og Sovjetunionen. Dette har medført nye måter å studere ”sikkerhet” på, og flere forskere ønsker å utvide sikkerhetsbegrepet til også å omfatte miljø, politikk, kultur og økonomi.

Nyrealistene mener fortsatt at nasjonal sikkerhetspolitikk først og fremst dreier seg om trusler rettet mot statens territorium, framsatt av aktiviteter fra en annen stat (Lipschutz 1995:5). Andre trusler kan eksistere, men de er ikke *sikkerhetstrusler*. Sikkerhet er et ord med mange betydninger, og det har vært stor uenighet om hva som ligger i begrepet og om det er nødvendig med en ”redefinering” av begrepet. I en artikkel i *Foreign Affairs* i 1989 (ibid.) skrev Jessica Tuchman Matthews at den globale utviklingen fører til et behov for å inkludere ressurs-, miljø- og demografiske saker i nasjonal sikkerhet. De ulike diskusjonene rundt ”hva er sikkerhet”, ”må sikkerhet redefineres” osv. har ført til en endring i hva stater oppfatter som sikkerhetspolitiske utfordringer. Statene påvirkes av den pågående forskningsdebatten og diskursen rundt begrepet sikkerhet. I følge Wæver innebærer en redefinering av sikkerhet ”a process of bringing *into* the field of security those things that, perhaps, should remain outside”(Lipschutz 1995:9). Dette vil være blant annet miljømessige og økonomiske trusler.

Buzan (1997:13) skriver at i følge den tradisjonelle militær-politiske forståelsen av sikkerhet handler sikkerhet om ”overlevelse”. Trusler kan oppstå på mange ulike områder, både militære og ikke-militære, men de må møte bestemte kriterier for å regnes som en sikkerhetssak. Dette er knyttet til begrepet sikkerhetisering. Truslene må ses på som eksistensielle trusler mot et referanseobjekt av en

---

[4] Heretter blir det fornorskede ”sikkerhetisering” brukt om Københavenrskolens begrep ”securitization”. Enkelte steder i oppgaven kan oversettelsen”det å gjøre noe til et sikkerhetsanliggende” forekomme, der dette bedre forklarer det som drøftes.

sikkerhetiserende(”securitizing”) aktør (ibid.). Referanseobjektet må ikke nødvendigvis være staten som man tradisjonelt har hevdet, men kan også være nasjoner, individer m.fl. ”In other words, issues become securitized when leaders (whether political, societal, or intellectual) begin to talk about them – and to gain the ear of the public and the state – in terms of existensial threats against some valued referent object” (Buzan 1997:13-14). Københavnerskolen er opptatt av å vise viktigheten av å flytte nye temaer eller saker inn på sikkerhetsagendaen og kaller dem dermed ”sikkerhetssaker”(Wæver 1995:75).

Siden temaet for oppgaven er cyber*terrorisme* ville det vært naturlig å gi plass til teorier innen terrorismeforskning i teorikapittelet. I utgangspunktet hadde jeg tenkt å ha en todeling av teori i denne oppgaven, nærmere bestemt å bruke *både* Københavnerskolens rammeverk og to teorier innen terrorismeforskning. Dette ville imidlertid blitt alt for omfattende i forhold til denne oppgavens ramme, og jeg har derfor valgt å holde meg til én teoretisk tilnærming; Københavnerskolen. To teorier som kunne belyst oppgavens tema er den såkalte ”smitteteorien” går ut på at forekomster av terrorisme i ett land ofte leder direkte eller indirekte til mer terrorisme i andre land, samt at det er et gjensidig avhengighetsforhold mellom moderne massemedia og terrorisme selv om konsekvensene av forholdet er tvetydige. En annen retning kalles ”terrorismens økologi” og er knyttet til teknologi og terrorisme. Samfunnsmessige forandringer assosiert med modernisering har skapt nye forhold for terrorisme, og den teknologiske utviklingen har ført med seg nye og mer effektive våpen (disse kan for øvrig også øke kontra-terrorisme kapabilitetene til stater) (Lia & Hansen 2000).

1.2.2 Metode

Oppgavens problemstilling og teorivalg tilsier bruk av et kvalitativt undersøkelsesopplegg. Analysen baserer seg på antakelsen om at begrepet cyberterrorisme blir sikkerhetisert og satt på den sikkerhetspolitiske agenda på grunn av måten begrepet blir representert av ulike aktører i den politiske og akademiske

diskurs. Metoden som velges for gjennomføring av analysen er derfor *diskursanalyse*. Som følge av dette vil analyse av ulike dokumenter knyttet til bruk av begrepet cyberterrorisme stå sentralt i oppgaven. Diskursanalyse kan defineres som "analyse av språkbruk i en samfunnsmessig kontekst, med fokus på hvordan de ideer og begreper som produseres i denne konteksten tolker og er med på å forme (et visst utsnitt av) den samfunnsmessige virkeligheten" (Mathisen 1997:3). Det er sammenheng mellom teori og valg av metode i oppgaven i og med at både Buzan (1997) og Wæver (1995) er opptatt av konseptualisering av begrepet sikkerhet innen en sikkerhetsdiskurs. Wæver (1995:55) skriver også at sikkerhet kan ses på som en talehandling (speech act). Hva som er sikkerhetspolitiske utfordringer konstitueres i måten sikkerhet omtales på. Det blir her interessant å se på i hvilken grad cyberterrorisme kan regnes som en sikkerhetspolitisk utfordring og om begrepet kan sies å ha blitt sikkerhetisert etter en studie av diskursen rundt begrepet. Oppgavens problemstilling gjør det vanskelig å operasjonalisere i bakgrunnsvariabel og avhengig variabel. Jeg velger derimot operasjonalisering i to nivåer. Nivå 1 er "speech acts" med vekt på at det sies at sentrale verdier er truet, mens nivå 2 er fullstendig sikkerhetisering som går på at konkrete tiltak som i andre sammenhenger blir sett på som illegitime iverksettes.

1.3 Avgrensninger

Av hensyn til oppgavens omfang må analysen av diskursen rundt begrepet cyberterrorisme avgrenses[5]. Kildematerialet er innhentet fra midten av 1990-tallet til et par år ut i det nye milenniet. Analysen er avgrenset i tid ved å legge vekt på perioden før og etter år 2000 ettersom cyberterrorisme var et begrep som ble stadig mer etablert i løpet av disse årene i media, av politikere og i akademiske miljøer. Det var stor bekymring for om Y2K ville skape omfattende problemer for den globaliserte, teknologiske verden og man kunne lese om faren for et verdensomspennende elektronisk sammenbrudd. I kjølvannet av disse scenariene

[5] Avgrensningen av diskursen og kildebruk blir utdypet i kapittel 3.

vokste begreper som cyberterrorisme, cyberspace og informasjonskrigføring seg stadig sterkere og er derfor en interessant periode å studere. Det skjedde ingenting ved milenniumskiftet, men verden ble derimot rystet av terroraksjonene i USA den 11. september 2001. Terroristene kapret fly og brukte disse som våpen da de styrtet inn i flere bygninger. Dette var en helt ny aksjonsform blant terrorister, og forskere, politikere og journalister spurte seg om dette ville rokke på terroristers bruk av tradisjonelle våpen som bomber. Flere antydet at vi også ville kunne se en større bruk av cybervåpen blant terrorister ettersom de hadde gått til det skritt å benytte seg av fly som våpen. Kildematerialet som benyttes strekker seg derfor til ett års tid etter 11.september-angrepene.

Når det gjelder avgrensning i rom byr begrepet cyberterrorisme på avgrensningsproblemer siden det ikke finnes en ensidig definisjon, forståelse og bruk av begrepet. Det blir vanskelig å presisere rammene for hva som forstås som cyberterrorisme. Dette er en utfordring for oppgaven, men nettopp derfor har oppgaven et kapittel med begrepsavklaringer hvor ulike definisjoner på cyberterrorisme og liknende begreper presenteres. Én definisjon blir valgt som den gjeldende for analysedelen.

Oppgaven er videre avgrenset institusjonelt ved at jeg studerer den sikkerhetspolitiske diskurs. Innenfor denne rammen ser jeg på diskursen i de politiske, akademiske og delvis mediarelaterte fora. Tekstprodusentene er politikere, forskere og journalister, og tekstene (kildene) blir inndelt i nivåer etter dette.

1.4 Organisering av oppgaven

I kapittel 2 presenteres oppgavens teoretiske tilnærming og hvordan jeg vil bruke Københavnerskolens rammeverk for å gjennomføre analysen.. Kapittel 3 er viet til metodiske betraktninger og kildebruk. Diskursanalyse blir introdusert som metode for å samle inn data. Kapittel 4 består av begrepsavklaringer. Kapittel 5 handler om oppbyggingen av et potensielt trusselbilde. Talehandlinger som går på

trusselvurderinger gjort av de sikkerhetiserende aktørene og analyse av empiriske eksempler på hendelser som er blitt omtalt som cyberterrorisme, samt andre relevante cyberangrep, blir presentert. Kapittel 6 inneholder diskursanalysen av begrepet cyberterrorisme. En rekke sentrale momenter som hva er trusselen, vurdering av trusselen m.m. fra den akademiske og politiske diskursen blir drøftet. Hensikten med kapittelet er å vise de ulike sikkerhetiserende aktørenes talehandlinger og avslutningsvis drøfte om disse kan gi grunnlag for å svare på om cyberterrorisme har blitt sikkerhetisert.. Konklusjon og avsluttende betraktninger kommer i kapittel 7.

2. Teoretisk tilnærming

Den teoretiske tilnærmingen i oppgaven baseres på Københavnerskolens rammeverk og skal legge grunnlaget for analysen av om begrepet cyberterrorisme er blitt sikkerhetisert og satt på den sikkerhetspolitiske agenda. I den første delen av kapittelet ser vi nærmere på den nye sikkerhetsagendaen etter den kalde krigen (2.1). Deretter presenteres det teoretiske rammeverket i oppgaven, og i den forbindelse knytter jeg min problemstilling til teorien og viser hvordan jeg vil bruke rammeverket til å gjennomføre analysen (2.2.). Hvordan jeg vil gå fram for å analysere diskursen rundt begrepet cyberterrorisme illustreres med en figur hvor de ulike komponentene som vil stå sentralt i analysen presenteres (2.3).

2.1 Den nye sikkerhetsagendaen

2.1.1 Etter den kalde krigen – Tradisjonalistene vs Utviderne

Etter 1989 har den europeiske sikkerhetsagendaen forandret seg radikalt. Etter å ha levd i et bipolart internasjonalt system siden den andre verdenskrig førte kollapsen av Sovjetunionen til en "ny verdensorden". Det bipolare system gikk over til å bli et multipolart system med Nord-Amerika, EU og Japan som de dominerende kapitalistsentrene (Buzan 1995: 197). I tillegg har det tidligere sterke fokuset på militær frykt og trusler blitt tonet ned, nettopp på grunn av den strukturelle endringen i det internasjonale samfunnet.

De siste 20 år har det vært en levende og engasjerende debatt om sikkerhetsbegrepet. Den kalde krigen var preget av begreper som sikkerhetsspiral og sikkerhetsdilemma, og etter den kalde krigen oppstod et "sikkerhetsvakuum" som måtte fylles. Dermed vokste det fram en debatt mellom de som fortsatt holdt på de gamle begreper (tradisjonalistene) og de som ønsket å utvide sikkerhetsagendaen("the wideners" - utviderne). Tradisjonelt sett er sikkerhet knyttet nasjonen og nasjonalstaten, og

begrepet sikkerhet refererer til staten (Wæver 1995; Buzan 1993). I kjølvannet etter kommunismens fall ble det av flere åpnet for å innlemme andre saker i sikkerhetspolitikken enn de tradisjonelle militære. For mange falt den tradisjonelle sikkerhetstenkingen bort, og miljø, økonomi og andre samfunnsmessige saker ble oppfattet som stadig viktigere sikkerhetsspørsmål. I dette nye spenningsfeltet innen sikkerhetspolitikk kan framveksten av begrepet cyberterrorisme plasseres. Når man ikke hadde "øst-vest truslene" å bekymre seg over fant man nye. Sterk vekst innen IT, økt globalisering og samhandling over store deler av verden har skapt grobunn for nye farer og trusler. Spesielt de industrialiserte statene har gjort seg svært avhengige av datateknologi i styringen av samfunnsvitale infrastrukturer, og dermed blir de sårbare for dataangrep fra ulike grupper aktører. I denne konteksten har frykten for cyberterrorisme vokst seg sterk og opptar stadig flere innen forskning, politikk og media.

Utviderne ønsket å utvide sikkerhetsagendaen til ikke bare å dreie seg om militære trusler, men også til å omfatte saker av økonomisk, politisk, miljømessig og samfunnsmessig karakter, mens tradisjonalistene insisterte på å knytte sikkerhet til militære konflikter. Tradisjonalistene ble kritisert av utviderne for å ha for snevert fokus, være statssentrert og som sagt, opptatt av militære aspekter. Utviderne derimot ble kritisert for å utvide sikkerhetsbegrepet *for* mye, at de kalte "alt" sikkerhet.

Etter den kalde krigen har teoretisk litteratur innen sikkerhetsstudier vært preget av tradisjonalistene, som har et sterkt militært fokus, utviderne, som ønsker å utvide sikkerhetsagendaen til å omfatte mer enn bare militær sektor, og kritiske sikkerhetsstudier som setter spørsmålstegn ved hele rammeverket sikkerhet omfattes av. På midten av 1980-tallet begynte rivaliseringen mellom de to store supermaktene USA og Sovjetunionen å avta, og flere av verdens fremtredende stater anså etter hvert sjansen for krig mellom de mektigste statene som svært liten. I tillegg startet en sikkerhetisering av tidligere sektorer som hadde blitt ansett som "low politics": miljø og økonomi. Fra 1960-tallet fikk man økt fokus på menneskets påvirkning av naturen og miljøet (f.eks. klimaendring og forurensning), og ønsket om å sikkerhetisere

miljøet for å bevare det ble sterkere. På grunn av økonomisk nedgang i USA og økende liberalisering av verdensøkonomien, startet også en sikkerhetiseringsprosess i den internasjonale økonomien (Buzan 1997:7). Debatten mellom tradisjonalistene og utviderne vokste fram på grunn av at noen var misfornøyd med det strenge militære fokuset som preget den kalde krigen, og når miljø og økonomi ble satt på den sikkerhetspolitiske agendaen fra 1960-tallet og utover, skapte det etter hvert motsetninger mellom de som ønsket denne utvidelsen, og de som ville bevare det militære fokus. Tradisjonalistene var redd for begrepet sikkerhet ville miste noe av sin betydning dersom ikke-militære saker skulle få status som sikkerhetsspørsmål (Buzan 1997:9). Stephen Walt har et strengt tradisjonalistisk syn og mener at sikkerhetsstudier handler om krig og at de kan defineres som ”the study of the threat, use, and control of military force”(Buzan m.fl. 1998:3). Han mener at ved å utvide agendaen for sikkerhetsstudier mister de sin intellektuelle sammenheng (”intellectual coherence”), og han tillater f.eks. at økonomi legges til agendaen bare hvis de kan relateres til militære saker (Buzan m.fl. 1998:3-4). Utviderne ble betegnelsen på de som mente at sikkerhet beskrevet i militære termer er for snevert for å beskrive de aktuelle sikkerhetsutfordringene.

En av de nye diskursene rundt begrepet ”sikkerhet” resulterte i en retning som kalles ”Københavnerskolen”, anført av blant annet forskerne Ole Wæver og Barry Buzan. Denne skolen har utviklet seg fra utviderne og tar for seg sikkerhetens fem primærsektorer: økonomisk, politisk, samfunnsmessig, militær og miljømessig. De forsøker å studere sikkerhet som noe mer enn bare en trussel ved at de setter trusler i sammenheng med referanseobjekter og ser på sikkerhetisering av disse truslene. I tillegg er skolen orientert rundt et ”talehandlingsperspektiv” og er opptatt av ”securitization” (heretter sikkerhetisering). I føle denne skoleretningen kan saker gjøres til sikkerhetssaker gjennom språkbruk, såkalte talehandlinger (speech act).

Ole Wæver (1995:55) skriver:

”In this usage security is not of interest as a sign that refers to something more real; the utterance itself is the act. By saying it, something is done (as in betting, giving a promise, naming a ship). By uttering “security”, a state representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it.”

2.1.2 Hva er sikkerhet?

Før man beveger seg inn på en diskusjon om *sikkerhetisering* er det nødvendig å kommentere hva som menes med *sikkerhet*. Sikkerhet er et komplekst begrep og forskere har stått overfor en utfordring for å komme fram til en klar definisjon av begrepet, og kanskje av den grunn har begreper som makt og fred ofte blitt brukt framfor sikkerhet i internasjonal politikk. I tradisjonell tenkning innen internasjonal politikk brukes begrepet sikkerhet om *overlevelse* (Buzan 1997: 13) og ”freedom from threat” (Buzan 1991:18). Sikkerhet handler om å opprettholde en stat og bevare borgernes rettigheter og identitet. Trusler kan oppstå på mange ulike områder, både militære og ikke-militære, men de må møte bestemte kriterier for å regnes som en sikkerhetssak. Dette er knyttet til begrepet sikkerhetisering. Truslene må ses på som eksistensielle trusler mot et referanseobjekt av en ”sikkerhetiserende”(securitizing) aktør (ibid.). Referanseobjektet må ikke nødvendigvis være staten som man tradisjonelt har hevdet, men kan også være nasjoner, individer, regjering, samfunn m.fl.

Wæver (1995:49) mener at sikkerhet må betraktes som nasjonal sikkerhet fordi verken individuell eller internasjonal sikkerhet eksisterer som begreper. Det konseptuelle fokus i hans timeglass-modell er statssuverenitet som ligger på nasjonal(stat)nivå, og det ligger mellom internasjonal og individuell *dynamikk* (ordet sikkerhet brukes ikke her).

Det finnes ulike tilnærminger til sikkerhetspolitikk innen internasjonal politikk og enkelte teoretikere drøfter om det er den samme betydningen av begrepet sikkerhet

som brukes, eller om de bare bruker det samme *ordet*, sikkerhet, men har ulik oppfatning av det og tillegger det forskjellig betydningsinnhold (Baldwin 1997: 59). I følge tradisjonell politisk-militær tenkning handler sikkerhet om *krig*. Referanseobjektet er ens egen stat som blir utsatt for krigstrusler fra andre stater. For å øke sitt lands sikkerhet må man øke sin evne til å forsvare seg med militære midler. Under den kalde krigen var den politisk-militære tilnærmingen den sentrale i og med all fokuseringen på sentral statsmakt, trusler, kontroll og militære strategier. Fra 1970-tallet og utover har den snevre sikkerhetstenkningen blitt utvidet av teoretikere som mener at ikke-statlige komponenter bør innlemmes i sikkerhetsdebatten, som saker av f.eks. miljømessig, samfunnsmessig og politisk karakter.

2.2 Københavnerskolens sikkerhetspolitiske rammeverk

2.2.1 Københavnerskolen

Merkelappen *Københavnerskolen* stammer fra en artikkel av en av skolens kritikere, Bill McSweeney (1996). Denne skoleretningen representerer ”utviderne” og tar utgangspunkt i de fem sektorene Buzan skisserte i sin bok fra 1991, *People, States & Fear*. De mest sentrale publikasjonene innenfor denne skolen kommer fra de mest fremtredende forskerne Buzan og Wæver, som siden 1988 har drevet forskning som går på redefinering av sikkerhetsbegrepet ved Copenhagen Peace Research Institute (Buzan 1997: 26). Jeg velger å vektlegge rammeverket som er skissert i Buzan m.fl. (1998). Forfatternes målsetning er å gi en klassifisering på: ”…what is and what is not a security issue, to explain how issues become securitized, and to locate the relevant security dynamics of the different types of levels ranging from local through regional to global.” (Buzan m.fl. 1998:1) Københavnerskolen bygger på Ole Wævers (1995) ideer om sikkerhet forstått som talehandling hvor revideringen av sikkerhetsbegrepet er basert på en diskursteoretisk tilnærming. Buzan m.fl.(1998:25) skriver:”The way to study securitization is to study discourse and political constellations.” Denne skolen knytter dermed teori og metode (sikkerhetiseringsteori og diskursanalyse) sammen på

en helt spesiell måte, og som vil være et fruktbart utgangspunkt for denne oppgavens problemstilling.

2.2.2 Sikkerhetisering

Sikkerhetisering kan bli sett på som en mer ekstrem form for politisering, og er direkte knyttet til diskurs og politiske konstellasjoner.

”Security is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Securitization can thus be seen as a more extreme version of politicisation. In theory, any public issue can be located on the spectrum ranging from nonpoliticized (…) through politicized (…) to securitized “(Buzan m.fl. 1998:23).

”Securitized”, eller sikkerhetisert, betegner en prosess der en sak blir presentert som en eksistensiell trussel som legitimt krever ekstraordinære tiltak som går utenfor vanlige politiske prosedyrer (Buzan m.fl. 1998:24). Saker blir sikkerhetisert når en *sikkerhetiserende aktør* får uttrykt seg på en slik måte at trusselen aktøren ytrer seg om blir oppfattet som så eksistensiell at både aktøren selv og dens tilhørere aksepterer de midlene som må til for å stoppe trusselen (selv om disse vanligvis er regler borgerne må respektere). Buzan m.fl.(1998:25) sier det slik: “If by means of an argument about the priority and urgency of an existensial threat the securitizing actor has managed to break free of procedures or rules he or she would otherwise be bound by, we are witnessing a case of securitization.”

Forfatterne innen Københavnerskolen er opptatt av *prosesser* som gjør en sak eller et fenomen til et sikkerhetsspørsmål, og det er denne prosessen som er *sikkerhetisering*. Det vil si at sikkerhetisering betraktes som en *bevegelse* i og med at det er ”securitizing move” [6] som er i fokus og som er et bilde på at en sak flyttes fra ”low” til ”high” politics. ”A discourse that takes the form of presenting something as an

[6] Kan oversettes til ”sikkerhetiserende handling”, men jeg velger å holde meg til det engelske begrepet.

existential threat to a referent object does not by itself create securitization – this is a *securitizing move*, but the issue is securitized only if and when the audience accepts it as such" (Buzan m.fl. 1998:25). Og videre: "If no signs of such acceptance exist, we can talk of only a securitizing move, not of an object actually being securitized" (ibid.). Dette er et viktig aspekt som må tas i betraktning i analysekapitlene.

For å finne ut om sikkerhetisering finner sted må vi studere prosesser. I den forbindelse er det viktig å skille mellom det Københavnerskolen kaller "a securitizing move" og "successful securitization". Det vil si skillet mellom forsøket på å få en sak til å bli oppfattet som en sikkerhetssak/trussel, og en vellykket sikkerhetiserende handling som tilsier at andre aksepterer saken som en sikkerhetssak. De sikkerhetiserende aktørene kan ikke sikkerhetisere alene. For å få flyttet en sak opp på den sikkerhetspolitiske agenda gjennom "a securitizing move" ved hjelp av en talehandling, er aktørene avhengig av at publikum oppfatter og godtar forståelsen av saken talehandlingen dreier seg om. Sannsynligheten for suksess vil påvirkes av ytre påvirkninger ettersom publikums vilje til å akseptere talehandlingene er avhengig av omgivelsene de befinner seg i. Dersom aksept fra publikum ikke er til stede ser vi kun et eksempel på "securitizing move" og *ikke* en vellykket *sikkerhetisering*, eller en såkalt fullstendig sikkerhetisering.

Buzan m.fl. (1998:39) skriver videre at det finnes sosialt definerte begrensninger på hva som kan og hva som ikke kan bli sikkerhetisert, men disse begrensningene kan endres. Cyberterrorisme er et relativt nytt begrep som ikke har blitt knyttet til teori i særlig stor grad. Jeg vil forsøke å sette begrepet inn i en sikkerhetiseringskontekst – kan det sies å ha blitt sikkerhetisert? Eller kan man rett og slett si at begrepet har blitt desikkerhetisert (at det ikke lenger regnes som en eksistensiell trussel av alvorlig karakter) fordi det har blitt kommentert så ofte og lagt fram som en eksistensiell trussel, men ingen alvorlige eksempler av eksistensiell art som har krevd spesielle tiltak har blitt rapportert? Dette rammeverket er først og fremst et verktøy som brukes til å vise hvordan forståelsen av sikkerhetsbegrepet kan utvides, men det kan også benyttes for å s på den motsatte prosess, såkalt desikkerhetisering. Det innebærer at

man flytter en sak som skaper konflikt ned ett nivå ved hjelp av diskursen slik at man kan gå tilbake til normal krisehåndtering med vanlige midler framfor å bruke ekstraordinære tiltak. Man forsøker med andre ord å flytte en sak ut av den sikkerhetspolitiske diskursen. Dette aspektet vil det tas hensyn til i analysen hvor vi skal forsøke å finne ut om cyberterrorisme har blitt sikkerhetisert.

Denne oppgaven er et forsøk på å knytte cyberterrorisme til Københavnerskolens sikkerhetsteori. Sikkerhetiseringsstudier har som mål å få klarhet i hvem som sikkerhetiserer, hvilke saker (trusler), for hvem (referanseobjekter), hvorfor, med hvilke resultater og under hvilke forhold (Buzan m.fl. 1998:32). Disse begrepene vil bli brukt videre i analysen.

2.2.3 Speech act

Talehandlingsperspektivet til denne sikkerhetstilnærmingen krever i følge Buzan m.fl. (1998) tre enheter i sikkerhetsanalysen: referanseobjekter, sikkerhetiserende aktører og funksjonelle aktører. En ”speech act” er en talehandling, og det er nettopp ytringen i seg selv som er handlingen (Wæver 1995:55). Gjennom bruken av ordet blir en sak gjort til et sikkerhetsanliggende. Det viktigste er om en sak blir presentert som en eksistensiell trussel og at publikum oppfatter den som sådan, ikke om trusselen er reell eller ikke. Oppfatninger, snarere enn realiteter, står i fokus. Likevel må det påpekes at talehandlingen ikke kun defineres ved å ytre ordet *sikkerhet*. Det som er essensielt er utpekelsen av en eksistensiell trussel som krever umiddelbar handling eller spesielle tiltak og at et publikum godtar utpekelsen (Buzan m.fl. 1998:27). Siden det her er fokus på ytring, relateres det direkte til diskurs, og den metodiske tilnærmingen i oppgaven er derfor *diskursanalyse*. I stedet for å konsentrere meg om ytringer om ordet *sikkerhet*, vil jeg se på talehandlinger som omfatter begrepet *cyberterrorisme* i ulike utvalgte diskurser. Dette for å se i hvilke kontekster ytringer om cyberterrorisme finnes, og for å finne ut av hvem og i hvilke fora cyberterrorisme eventuelt kan sies å ha blitt *sikkerhetisert*.

2.2.4 Referanseobjekt

Etter den kalde krigen har mange samfunnsproblemer blitt forsøkt knyttet til sikkerhetsbegrepet; fattigdom, ressursmangel, kriminalitet, forurensning m.m. Buzan (1991:19) hevder at sikkerhet hovedsakelig er betinget av faktorer i fem sektorer: militære, politiske, økonomiske, samfunnsmessige og miljømessige. Hver av disse faktorene har et fokus innenfor sikkerhetsproblematikken og har hver sine referanseobjekter. Cyberterrorisme kan ikke plasseres i én av disse kategoriene, men kan "fordeles" over flere. *Referanseobjekt* defineres som ting som blir sett på som eksistensielt truet og som har legitimt krav til overlevelse (Buzan m.fl.1998:36). Jeg vil hevde at jeg kan relatere dette aspektet ved den teoretiske tilnærmingen til cyberterrorisme. Tradisjonelt sett har referanseobjektet for sikkerhet vært staten (realistisk syn). Innenfor de ulike sektorene som utviderne og Københavnerskolen nevner, er staten fortsatt det viktigste referanseobjekt i militær sektor, i politisk sektor er det de grunnleggende prinsippene ved staten som suverenitet og av og til ideologi, og i samfunnsmessig sektor er det kollektive identiteter som kan fungere uavhengig av staten, som nasjoner og religioner, som er referanseobjekt. I økonomisk og miljømessig sektor er det verre å definere et bestemt referanseobjekt. I økonomisk sektor kan det nevnes at f.eks. firmaer er truet av konkurs, og innen miljømessig sektor kan mulige referanseobjekter være overlevelse av truede arter og bevaring av klima (Buzan 1997: 16-17). Man kan med andre ord hevde at staten som kjernereferanseobjekt har endret seg, og Københavnerskolen åpner for at det finnes andre referanseobjekter enn nettopp staten. Nasjoner, individer, regjering, samfunn m.fl. kan også være referanseobjekter. "In other words, issues become securitized when leaders (whether political, societal, or intellectual) begin to talk about them – and to gain the ear of the public and the state – in terms of existensial threats against some valued referent object" (Buzan 1997:13-14). Københavnerskolen er opptatt av å vise viktigheten av å flytte nye temaer eller saker inn på sikkerhetsagendaen og kaller dem dermed "sikkerhetssaker"(Wæver 1995:75).

Mange teoretikere ser på individer som referanseobjekter for sikkerhet, men det er diskusjoner om på hvilken måte og i hvilken grad staten kan sikre sine individer. Staten kan ses på som en trussel til individets sikkerhet i seg selv. Med *cyberterrorisme* som fokus hevder jeg at det er mulig å bruke kritisk infrastruktur (transport, tele- og kraftforsyning, bank- og finansinstitusjoner og ulike datasystemer) som referanseobjekt (se figur 1). Jeg mener det går an å bruke Buzans tilnærming her i og med at disse ovennevnte sakene kan bli sett på som eksistensielt truet (av f.eks. virus, hacking og annen datainntrengning samt fysisk sabotasje og ødeleggelse) og som har legitim rett til overlevelse (samfunnet er avhengig av disse funksjonene). Disse samfunnsfunksjonene må bestå for å bevare staten og dens borgeres selvopprettholdelse. Uten fungerende infrastruktur vil samfunnet resultere i kaos. I den nye sikkerhetsagendaen er staten som sagt mye mindre viktig enn tidligere selv om den fortsatt har en sentral rolle, men nye referanseobjekter og kilder for trusler har kommet i tillegg til staten (Buzan 1997:11). Med henvisning til dette utsagnet mener jeg at det vil være mulig å bruke de referanseobjektene jeg har nevnt ovenfor. Det bør likevel nevnes at det ikke nødvendigvis må være et skille mellom staten og kritisk infrastruktur som referanseobjekt. Transformeringen av staten er blant annet et resultat av IT-revolusjonen der statens evne til å opprettholde velferd og sikkerhet er avhengig av kritisk infrastruktur. Kritisk infrastruktur er mer sentral i opprettholdelsen av nasjonal sikkerhet enn før, og det *forventes* at avhengighet av IT-styrte infrastrukturer vil øke. Denne *forventningen* er svært sentral i diskusjonen om cyberterrorisme fordi ytringer i diskursen i stor grad går på hvilke trusler man forventer og dermed hvordan man oppfatter cybertrusselen. Forventningene og oppfattelsen av truslene som skapes rundt cyberterrorisme er med på å bestemme om cyberterrorisme blir sikkerhetisert, eller eventuelt desikkerhetisert.

2.2.5 Sikkerhetiserende aktører

Sikkerhetiserende aktører er aktører som sikkerhetiserer saker ved å definere noe – et referanseobjekt - som eksistensielt truet (Buzan m.fl. 1998:36). Jeg velger å betrakte forskere, politikere og journalister som sikkerhetiserende aktører fordi de setter

”agenda” for hva som kan oppfattes som en trussel mot et referanseobjekt. Buzan m.fl. (1998) nevner også funksjonelle aktører som er aktører som påvirker sektorenes dynamikk[7], men jeg vektlegger ikke disse aktørene da jeg ikke har spesielt fokus på sektorer i oppgaven. Funksjonelle aktører kan derimot ha en påvirkningskraft, i mitt tilfelle særlig med hensyn til en eventuell desikkerhetisering av cyberterrorisme. Det er den sikkerhetiserende aktøren (en person eller en gruppe) som kommer med ”speech act”, en talehandling, om sikkerhet. Vanligvis består aktørene av politiske ledere, regjeringer, lobbyister, pressgrupper osv. (Buzan m.fl. 1998:40), og jeg mener mitt valg av sikkerhetiserende aktører i så måte står i samsvar med den teoretiske tilnærmingen.

2.2.6 Hvorfor sikkerhetisere?

Generelt kan man si at grunnene til at man sikkerhetiserer har med aktørene å gjøre siden de er de som ytrer seg, skaper en oppfattelse av hva som er truet og dermed setter saker på den sikkerhetspolitiske agenda. Det er de sikkerhetiserende aktørene som definerer referanseobjektene, og det er de som taler sikkerhet på vegne av seg selv eller referanseobjektene. Sikkerhetisering vil si at man gjør noe til et sikkerhetsanliggende, og det er ulike årsaker til hvorfor aktørene sikkerhetiserer. Journalistene kan ha ønske om å være *den* personen som setter en ny og viktig sak på dagsordenen slik at deres renommé øker, eller de har bare ønske om skape publisitet og indirekte tjene penger. Forskere og politikere kan ha andre grunner til å sikkerhetisere, som f.eks. å skape blest om en forskningsstudie eller sette en sak på den politiske dagsorden og gjennomføre et konkret tiltak.

[7] Funksjonelle aktører er aktører som *påvirker* avgjørelser innen feltet sikkerhet, de er ikke referanseobjekter og er heller ikke de som sikkerhetiserer saker (Buzan m.fl. 1998: 36)

2.3 Sikkerhetisering av cyberterrorisme

I en sikkerhetiseringsprosess må ulike enheter som referanseobjekter, trusler og sikkerhetiserende aktører defineres for å kunne si noe om hvordan de påvirker sikkerhetiseringen. Buzan m.fl. (1998:172) undersøker Frankrikes sikkerhet ved hjelp av en figur og definering av de ovennevnte begreper i relasjon til staten Frankrike (som da er analyseenhet). Jeg vil forsøke å bruke denne figuren som utgangspunkt og ramme for analysen av diskursen rundt begrepet cyberterrorisme, se *figur 1*: *Sikkerhetisering av cyberterrorisme*. Jeg setter cyberterrorisme som analyseenhet, og som referanseobjekter setter jeg saker som kan bli eksistensielt truet og som må eksistere for at staten og borgernes velstand skal kunne opprettholdes. Siden cyberterrorisme er analyseenhet har jeg valgt referanseobjekter som vil være truet ved et eventuelt cyberterroristangrep[8] i følge diskursen innen dette feltet, nærmere bestemt ulike typer kritisk infrastruktur. Det er de sikkerhetiserende aktørene som definerer hvilke referanseobjekter som kan være eksistensielt truet. Det meste av diskursen innen cyberterrorisme og informasjonsoperasjoner foregår blant forskere, blant politikere og i media. På forskjellig måte setter disse agendaen for hva som er trusler og hvem som blir truet. Det er derfor disse som er oppført som sikkerhetiserende aktører i figuren. Forskerne forsker på f.eks. teknologi- og kommunikasjon, krigføring, terrorisme og data og ser hva som er mulig å gjøre og hvilke skader IT-utviklingen kan gjøre på kritiske samfunnsstrukturer. Politikere må ta forskningen til etterretning og eventuelt opprette undersøkelsesutvalg, komiteer, bestille offentlige utredninger, omgjøre lovverk m.m. De har også muligheten til å gjennomføre fullstendig sikkerhetisering av en sak gjennom å sette i gang ekstraordinære tiltak. Media får med seg hva forskerne finner ut og politikernes reaksjoner og kringkaster det for allmennheten. De sikkerhetiserende aktørene har enn oppfatning om at ulike former for virus, hacking og bruk av fysiske cybervåpen m.m. utgjør en trussel for samfunnets infrastrukturer og viktige datasystemer innen viktige samfunnsfunksjoner,

[8] Mange vil i stedet bruke cyberangrep som begrep.

samt at det får store konsekvenser hvis også det private marked blir berørt. Figuren gir et bilde på hvilke enheter som relateres til cyberterrorisme, og med denne som utgangspunkt vil det bli mulig å sortere de ulike diskursene innen emnet og forhåpentligvis si noe om begrepet cyberterrorisme har blitt sikkerhetisert og er en del av den sikkerhetspolitiske agenda.

Figur 1: Sikkerhetisering av cyberterrorisme

Navn	*Referanseobjekt*	*Trusler*[1]… i følge …	*Sikkerhetiserende aktører*
Cyber-terrorisme	Kritisk infrastruktur: *Transport* *Telekommunikasjon* *Kraftforsyning* *Bank og finans* *Forsvarets datasystemer* *Bedrifters datasystemer*	Hacking Virus EMP Jamming Spoofing Sniffing Trojansk hest Denial of service	Forskere (akademisk nivå) Politikere (politisk nivå) Journalister (media)

2.4 Oppsummering

Målet med dette kapittelet har vært å redegjøre for det teoretiske rammeverket som vil ligge til grunn for analysen i oppgaven. Staten har tradisjonelt vært sett på som referanseobjekt i sikkerhetstenkningen, men utover på 1980-tallet ble dette synet utfordret. En ny gruppe forskere hadde et utvidet sikkerhetsbegrep hvor man ikke

lenger satte militær sikkerhet og staten i sentrum, men hevdet at sikkerhet kunne omfatte mye mer. Københavnerskolen representerer det utvidete sikkerhetsperspektivet og åpner for ideen om at det kan finnes en rekke referanseobjekter for sikkerhet. Oppgaven vil forsøke å vise at det utvidete sikkerhetsbegrepet er til stede i diskursen rundt cyberterrorisme. Rammeverket benyttes til å klassifisere hvilke referanseobjekter som kan knyttes til cyberterrorisme, hva som oppfattes som trusler i forhold til cyberterrorisme, og hvem som snakker sikkerhet i forbindelse med cyberterrorisme. Dette oppsummeres i figur 1 som danner ramme for analysen i kapittel 5 og 6.

3. Metodiske betraktninger og kilder

”En metode er en framgangsmåte, et middel til å løse problemer og komme fram til ny kunnskap”(Hellevik 1991:14). Denne oppgaven søker å gå i dybden på debatten og diskursen rundt begrepet cyberterrorisme, og *diskursanalyse* blir derfor valgt som metodisk tilnærming og analyseverktøy. Ved å velge diskursanalyse som metode støtter oppgaven seg på Buzan m.fl. (1998) som hevder at sikkerhetisering er en prosess som best kan studeres ved å undersøke diskurser og politiske konstellasjoner (se 2.2). Problemstillingen tilsier at det er hensiktsmessig å bruke et kvalitativt analyseopplegg, som betyr at det legges vekt på å finne fram til den underliggende meningen i en tekst (Hellevik 1991:153). Valg av metode er betinget av forskerens mål med analysen. I dette tilfellet er målet med oppgaven å *beskrive* framveksten av cyberterrorisme som et begrep (derfor har oppgaven et kapittel med begrepsavklaringer, se kap. 4), *drøfte* om dette begrepet er blitt satt på den sikkerhetspolitiske agenda og om mulig blitt sikkerhetisert, og *forklare* hvilke mekanismer i diskursen (ved hjelp av sikkerhetiserende aktører, referanseobjekt m.m.) som fører fram til en konklusjon på hvordan cyberterrorisme blir oppfattet. Metodekapittelet begynner med en framstilling av diskursanalyse som metode (3.1), fulgt av avgrensning av diskursen (3.2) og drøfting av muligheter og begrensninger ved valg av denne metoden (3.3). Deretter blir det redegjort for kildebruk i oppgaven (3.4).

3.1 Diskursanalyse som metode

Det finnes mange definisjoner på diskursanalyse og begrepets betydning er omstridt i samfunnsvitenskapen. Diskursanalyse kan defineres som ”analyse av språkbruk i en samfunnsmessig kontekst, med fokus på hvordan de ideer og begreper som produseres i denne konteksten tolker og er med på å forme (et visst utsnitt av) den samfunnsmessige virkeligheten” (Mathisen 1997:3). Jørgensen & Phillips (1999:9) definerer diskurs som ”en bestemt måte å tale om og forstå verden (eller et utsnitt av

verden) på". Iver B. Neumann (2001:18) sier det på følgende måte: "En diskurs er et system for frembringelse at ett sett utsagn og praksiser som, ved å innskrive seg i institusjoner og fremstå som mer eller mindre normale, er virkelighetskonstituerende for sine bærere og har en viss grad av regularitet i ett sett sosiale relasjoner". Felles for de fleste definisjonene er uansett at "diskursanalyse handler om å analysere tekster eller språkbruk, betraktet som samfunnsmessig virksomhet og i sin samfunnsmessige kontekst" (Mathisen 1997:2)[9].

Spesielt Mathisens definisjon rommer *kjernen* i oppgaven; altså det at jeg vil analysere hvordan begrepet cyberterrorisme brukes i en samfunnsmessig kontekst med fokus på hvordan de begrepene og ideene som produseres i denne konteksten er med på å *tolke* og forme virkeligheten, altså hvordan diskursen er med på å skape oppfatninger om cybertrusselen. Diskursbegrepet omtales blant annet om å dekke alle former for talt interaksjon og skrevne tekster og å analysere sammenhengen mellom tekst og kontekst (Mathisen 1997:1-2). En grunn for å studere sosiale tekster er for å oppnå bedre forståelse av sosialt liv og sosial interaksjon. Måten man bruker språk på virker inn på samfunnsmessige og politiske relasjoner samtidig som språk formes og reguleres av sosiale og politiske strukturer og interesser. Språklige ytringer, ord, oppfattes ofte som mindre viktige enn handlinger, hva som gjøres betyr mer enn det som sies. Kanskje er dette riktig, men hva som sies før og etter en handling har store konsekvenser for hvilken betydning denne handlingen tillegges. Det er en nær forbindelse mellom ord og handling. Menneskelige handlinger blir styrt av meninger, og meninger er noe alle har og vi deler dem ved hjelp av språklige ytringer[10]. Ord som brukes, eller *ikke* brukes, kan få store konsekvenser i mange sammenhenger, politisk, juridisk og sosialt. "Å studere språklig kommunikasjon er nødvendig for å forstå

---

[9] Mathisen, Jørgensen & Philips og Neumann har en noenlunde lik definisjon av diskursanalyse, og det er disse som er hovedkildene mine for diskursanalyse. Jeg velger imidlertid å bruke Mathisens forskningsnotat (1997) som metodisk bakgrunn for analysen ettersom jeg mener hans redegjørelse for hva diskursanalyse er og hvordan diskursen kan avgrenses passer til mitt forskningsopplegg.

[10] "Mening" er et *vagt* ord som brukes om mye. En definisjon på *mening* er: "Tanke, fornuftig sammenheng" (www.storenorskeleksikon.no).

politiske aktører og deres handlinger" (Mathisen 1997:5). I tekster formes aktørenes preferanser og holdninger som er avgjørende for deres handlinger. Det er gjennom språklig kommunikasjon politikerne setter ulike saker på den politiske dagsorden. Diskursanalyse brukes til å belyse hvordan politiske saker defineres og fortolkes (ibid.:6).

3.2 Avgrensning av diskursen

Neumann (2001) skriver at første skritt i en diskursanalyse er å avgrense den diskursen man ønsker å studere. Andre skritt er å sette opp en inventarliste over de representasjoner som finnes i den valgte diskursen (det vil si formeninger om hvordan virkeligheten skal forstås). Tredje skritt går ut på å finne diskursens lagdeling og spørre seg om alle trekk ved den gitte representasjon er like bestandige. Mathisen (1997) er også opptatt av hvordan diskurser bør avgrenses, og det viktige er at de avgrenses etter det faglige utgangspunktet for og formålet med analysen[11]. Diskursen må relateres til sine kontekster og man må analysere hvordan disse virker inn på diskursen og hvilken funksjon denne fyller i en bestemt kontekst. Han går blant annet inn på institusjonelle avgrensninger av diskurser hvor utgangspunktet er bestemte samfunnsmessige virksomheter, som institusjoner og organisasjoner, og de institusjonelle rammene rundt disse. Her menes at man avgrenser politiske diskurser knyttet til politisk virksomhet og politikkområder; den miljøpolitiske, den samferdselspolitiske diskurs osv. Innenfor disse institusjonelle rammene er det mulig å si at jeg holder meg til den sikkerhetspolitiske diskurs. "En sikkerhetspolitisk diskurs" høres stor og omfattende ut, men man kan benytte seg av underdiskurser. Ved å bruke en institusjonell avgrensning får diskursanalysen en sosial forankring fordi vi opererer med en bestemt organisasjon og konteksten rundt denne organisasjonen.

---

[11] Neumann (2001) og Mathisen (1997) har delvis et likt syn på hvordan diskursen kan avgrenses, men jeg holder meg til Mathisens opplegg.

I følge Mathisen (1997) kan diskurser også avgrenses med utgangspunkt i diskursens produksjon, distribusjon og forbruk av tekst. ”Vi må da finne ut hvilke tekst-produkter og produsenter, distributører og forbrukere som kan sies å høre sammen og utgjøre ”diskursførende” sosiale nettverk”(Mathisen 1997:20). I mange tilfeller er det vanskelig å skille denne avgrensningen fra den institusjonelle fordi man i politiske systemer, institusjoner og organisasjoner også produserer tekster. Dette gjelder også i min diskursanalyse. Denne oppgaven har en institusjonell avgrensning i og med at jeg ser på den sikkerhetspolitiske diskurs, og det er tekster *produsert* av forskere og politikere og delvis journalister med sikkerhetspolitisk tema (nærmere bestemt cyberterrorisme, informasjonskrigføring og andre relaterte begreper) som er gjenstand for analyse. ”En avgrensning av en diskurs ut fra et nettverk av tekstprodusenter og tekstforbrukere vil langt på vei kunne falle sammen med en institusjonell avgrensning” (Mathisen 1997:20). Med andre ord, teksten og dens institusjonelle kontekst må skal ses i sammenheng.

Et videre avgrensningsspørsmål gjelder hvordan man finner ut hvilke tekster som hører sammen og utgjør en diskurs. Diskursen kan bestå av tekster produsert og distribuert innenfor en bestemt organisatorisk/institusjonell kontekst, et bestemt utvalg tekster produsert i et gitt tidsrom, alle tekster som omtaler eller handler om et bestemt fenomen m.m. Man må være bevisst på hvilke tekster man legger til grunn i diskursen, og det kan være mulig å ”avgrense en diskurs som en samling tekster som omtaler et eller flere fenomener på en bestemt måte”(Mathisen 1997:21). I denne forbindelse er det viktig å avgrense diskursen i *tid og rom*, men det kan selvsagt være vanskelig å fastlegge en slik avgrensning. Oppgaven presenterer et utvalg tekster fra ulike produsenter i et gitt tidsrom. Tekstene omhandler et bestemt fenomen; cyberterrorisme.

I forhold til avgrensning i *tid* tar analysen for seg tekster om cyberterrorisme hovedsakelig fra 1995 til 2003 (se 1.3). Oppgavens ramme tilsier at alle tekster der begrepet cyberterrorisme og relaterte ord og begreper er omtalt ikke kan tas med, men

det er foretatt et representativt utvalg (se 3.4). Analysen blir også avgrenset i *rom* ved at rammene for hva som forstås som cyberterrorisme må presiseres. Det har derfor vært nødvendig å innlemme et begrepsavklaringskapittel i oppgaven for å gjøre et forsøk på å definere cyberterrorisme og relaterte begreper (se kap.4). Nettopp fordi cyberterrorisme er et nytt og sammensatt begrep vil talehandlinger med relaterte begreper også tas med i analysen, selv om det er ytringer som omhandler selve cyberterrorismebegrepet som står i fokus og som skal danne hovedgrunnlag for å svare på problemstillingen. Relatert til tid og rom er også spørsmålene: ”Hva slags fora foregår diskursen i”, og ”hvem produserer tekstene” m.m. (Mathisen 1997:25-26). Dersom vi ser på *hvem* som produserer tekstene, blir vi tilført kunnskap om forfatterne som kan øke vår innsikt i hva som (ikke) fanges opp av diskursen. Når en diskurs har fått en bestemt vinkling og innretting, og når visse synspunkter har blitt toneangivende og etablert, virker det inn på rekrutteringen av nye diskursdeltakere. Hvordan diskursen blir påvirket av nye deltakere er avhengig av om de får delta på egne premisser, om de på forhånd har gjennomtenkte meninger om temaer i diskursen, hvilken bakgrunn de har osv. Det kan ligge begrensninger på hvem og hva som slipper til i diskursen.

”Hvem produserer tekstene” kan overføres til ”hvem er de sikkerhetiserende aktørene”. Som nevnt i teorikapittelet vil analysen se på forskere og politikere og journalister som sikkerhetiserende aktører, og det er disse aktørene som produserer tekst med talehandlinger knyttet til cyberterrorisme. ”Fora diskursen foregår i” blir dermed de politiske og akademiske (og til dels mediarelaterte) fora innenfor en sikkerhetspolitisk institusjonell ramme. I analysen blir tekstene delt inn etter hvilket ”nivå” de ligger på i form av kildemateriale utgitt i akademiske og politiske kretser. Det etableres med andre ord en sammenheng med *hvem* som produserer tekster og den en bestemt organisatorisk/institusjonell kontekst. Med en slik inndeling vil det være mulig å se nettopp i hvilke fora diskursen foregår i og om begrepet endrer seg etter hvilket fora det ”behandles” i, og da naturligvis *hvilke* mennesker som drøfter det og skriver om det. Det finnes svært mye dokumentasjon fra media i form av

avisartikler og internettartikler. Da disse som regel gjengir uttalelser eller beskriver dokumenter, artikler og rapporter skrevet av akademikere, politikere og byråkrater, kan ikke media brukes som eget ”nivå” i analysen, men journalister regnes som sikkerhetiserende aktører og man kan snakke om et mediarelatert fora. Det er nevnt ovenfor at man kan avgrense en diskurs som en samling tekster som omtaler et eller flere fenomener på en bestemt måte. I denne oppgaven blir tekster som omtaler ”fenomenet” *cyberterrorisme* gjenstand for analyse, men også en del tekster med relaterte begreper.

3.3 Muligheter og begrensninger ved diskursanalyse

Det er flere problematiske aspekter ved bruk av diskursanalyse som metode i studiet av cyberterrorisme, men det er også mye som tyder på at diskursanalyse er egnet til å belyse oppgavens problemstilling. En diskursanalyse av cyberterrorisme vil ikke resultere i definitive svar, men en analyse av diskursen rundt begrepet vil tilføre leseren ny forståelse av hva cyberterrorisme er og betyr i en sikkerhetspolitisk kontekst. Det er også en fare for at forskeren tillegger diskursen for stor betydning og tolker for mye ut av tekstene. Man kan risikere å se sikkerhetspolitiske aspekter og trusler i hvert dokument som omhandler cyberterrorisme, blant annet fordi begrepet i seg selv er såpass *ladet*, slik at man setter utsagn om cyberterrorisme inn i en sikkerhetiseringskontekst uten å drøfte talehandlingen godt nok. Forskeren må alltid ha i minne det teoretiske rammeverket som påpeker forskjellen på ”a securitizing move”, sikkerhetisering og politisering. Dette for å hindre feiltolkning av kildene. Man kan heller ikke være sikker på om folk virkelig mener det de sier og om de handler slik de sier. Problemstillingen legger ikke opp til at man skal studere aktørenes intensjoner, men at man vil vite hvordan diskursen forløper, og dermed er ikke dette et problem i denne oppgaven. Utsagn fra de ulike diskursene er hyppig gjengitt i analysen, og analysen består av en rekke sitater som drøftes. Dette styrker kravet om etterprøvbarhet.

Reliabilitet og validitet må kommenteres i forbindelse med diskusjon om metode og operasjonalisering av variabler. Reliabilitet henspeiler på nøyaktigheten i målingene som gjøres og er forbundet med kildene og deres pålitelighet, mens validitet sikter til datas relevans for problemstillingen i oppgaven (Hellevik 1991:159). Lav validitet vil si at man ikke har undersøkt det man sier man skal undersøke. Datas validitet henspeiler på samsvaret mellom den teoretiske definisjonen og den operasjonelle definisjonen som styrer datainnsamlingen (Østerud m.fl.1997: 285). Med denne problemstillingen har det har vært vanskelig å operasjonalisere siden det ikke er *konkrete* variabler å forholde seg til. Jeg har derfor valgt operasjonalisering i to nivåer, "speech acts" og fullstendig sikkerhetisering (se 1.2.2). I tillegg blir begrepene brukt konsekvent og på lik måte både på empiri- og teoriplanet, og slik er det prøvd å oppnå høy grad av definisjonsmessig validitet. Cyberterrorisme ses på som en enhet i analysen, men det blir vanskelig å lage en modell over ulike variabler og deres påvirkning på hverandre, og det er som nevnt valgt nivåer i stedet. Det er nettopp en analyse av selve diskursen rundt begrepet som blir hoveddelen i analysen, og da kan ikke cyberterrorisme defineres klart på forhånd. Det legges imidlertid en figur (se 2.3) til grunn for analysen også som viser sammenhengen mellom ulike faktorer i forbindelse med sikkerhetisering av cyberterrorismebegrepet. Når det gjelder reliabilitet henspeiler det ikke bare på kildenes troverdighet, men også hvordan man bruker kildene; det skal være samsvar mellom den operasjonelle definisjonen og data. I denne oppgaven står kildene, og nettopp *bruken* av kildene svært sentralt siden metoden som brukes er diskursanalyse, og det er mye som tyder på at kravet om høy reliabilitet blir oppnådd.

3.4 Kildebruk

Oppgaven baseres på ulike typer kilder som bøker, forskningsrapporter, tidsskriftartikler, avismateriale, offentlige dokumenter, konferansepapers og diverse "funn" på Internett, det være seg uoffisielle publikasjoner, debattinnlegg m.m. Kildene er delt inn i publikasjoner fra forskning/akademisk miljø, politisk miljø og

media, i tråd med samme inndeling som følges i analysen hvor drøftingen legges på ulike "nivåer" (se 6.1 hvor jeg drøfter medias rolle og velger å innbefatte mediediskursen som en del av både det akademiske og politiske nivå). Det gjøres oppmerksom på at en rekke dokumenter er lastet ned fra Internett, og det finnes i mange tilfeller ikke sidetallshenvisninger på artikler, offentlige dokumenter osv. som ligger på nett.

3.4.1 Akademisk miljø

En undersøkelse av diskursen i det akademiske miljø innebærer at man må se hvor forskningen på dette feltet foregår og hvem som forsker på temaer relatert til cyberterrorisme og som skriver artikler, bøker o.l. om det. Det har selvfølgelig vært nødvendig å foreta et *utvalg* av akademiske kilder. Fokuset i litteratursøkingen har vært å finne ytringer i det skriftlige og muntlige materialet som går på synspunkter, vurderinger og kommentarer til trusselen knyttet til cyberterrorisme og relaterte begreper. Jeg startet søkingen på Internett for å finne navn på personer og forskningsinstitusjoner som driver forskning knyttet til cyberterrorisme. Jeg har deretter kunnet finne bøker, tidsskriftartikler og forskningsrapporter, notater og konferansepapers fra en rekke forskere. Norge har ikke kommet spesielt langt innen forskning på cyber-relaterte spørsmål, men interessen for dette forskningsfeltet har økt. Spesielt etter terrorangrepene i New York 11. september 2001 har det blitt økt fokus på muligheten for at terrorister også kan komme til å benytte seg av cyberterrorisme, nett-terrorisme o l. Siden Norge er et høyteknologiland, har flere og flere påpekt hvor sårbart samfunnet angivelig har blitt og har dermed vunnet gjennomslag for nødvendig forskning innen dette feltet. Forsvarets Forskningsinstitutt (FFI) har en forskningsserie, TERRA[12], som blant annet studerer en rekke ulike forhold knyttet til terrorisme, inkludert cyberterrorisme. Sentrale terrorismeforskere i Norge er Tore Bjørgo, Politihøgskolen og NUPI, og Jan Oskar Engene, UiB, og

[12] Den mest sentrale terrorismeforskeren ved FFI er Brynjar Lia, men også flere forskere ved instituttet, som Thomas Hegghammer og Petter Nesser, har gjort seg bemerket den senere tid.

Brynjar Lia, FFI, men ingen av disse har konsentrert seg om cyberterrorisme. Foruten FFI har flere deler av Forsvaret prosjekter som behandler informasjonsoperasjoner, som er et av begrepene som relateres til cyberterrorisme. Disse institusjonene har også prosjekter på elektronisk krigføring og psykologiske operasjoner (*psyops*), men dette går ofte inn under informasjonsoperasjoner, som av mange brukes som en samlebetegnelse.

Det meste av forskningen på cyberterrorisme drives i USA. Siden det ikke finnes mye norsk litteratur på emnet, så de er mest sentrale kildene amerikanske. I USA har disse temaene vært på dagsordenen så å si etter Golfkrigen og det er opprettet flere forskningsinstitutter som analyserer den nye typen trusler; National Infrastructure Protection Center (NIPC) og Computer Security Institute for å nevne noen. Ved flere amerikanske universiteter, som Georgetown University og National Defense University, er det også miljø for forskning innen cyber-relaterte spørsmål. Dorothy Denning, Martin Libicki, Mark Pollitt, John Arquilla og David Ronfeldt er et utvalg navn som går igjen i forskningslitteraturen og på konferanser, og jeg har derfor brukt disse i stor utstrekning. Det at det er mange av de samme kildene som går igjen er et interessant aspekt i diskursanalysen.

Selv om USA er størst på denne type forskning, har også andre land begynt å fokusere på cyberproblematikken i større grad enn før. I land som Sverige, Tyskland, England, Kina og Russland rører det seg i forskningsmiljøene[13]. I Sverige har Totalförsvarets Forskninsinstitut (FOI) vært involvert i forskning rundt cyberspørsmål i flere år. Russerne er opptatt av informasjonspsykologiske og militærtekniske aspekter ved informasjonskrigføring, men det er særlig det første som står i fokus. Kineserne utnytter sine tekniske kapabiliteter også i moderne krigføring, og det har kommet flere uttalelser fra høyt hold i Kina om at Kina må forberede seg på en framtidig cyberkrig og er åpne for å bruke cybervåpen i konflikter med sine fiender.

---

[13] Se blant annet Grunnan (2000) for mer informasjon om tiltak og forskning i de nevnte landene.

3.4.2 Politisk miljø

Det finnes få rene politiske dokumenter som omhandler cyberterrorisme. Her har det derfor vært aktuelt å gå litt utenfor definisjonen på cyberterrorisme for å se hva som rører seg i den politiske diskursen rundt relaterte begreper som terrorisme, cyberspace, datakriminalitet m.v. Av norske dokumenter er det særlig NOU'er og Stortingsmeldinger som omhandler trusler og sikkerhet i forbindelse med forsvar og samfunnssikkerhet (og deriblant terrorisme) som har vært gjenstand for analyse. Det vil gå ut over oppgavens omfang å bruke offentlige og politiske dokumenter fra et stort utvalg forskjellige land. I tillegg til de norske dokumentene tar derfor oppgaven for seg utvalgte (de som har vært lettest tilgjengelige, og dokumenter med stor medieomtale) politisk-administrative dokumenter fra USA og Europa (både EU-dokumenter og dokumenter fra Europarådet).

3.4.3 Media

Det finnes *svært mange* artikler, referater og kommentarer i media som handler om cyberterrorisme, informasjonskrigføring, cyberspace, hacking osv. Oppgavens omfang gjør at det er begrensninger for hvor stort utvalget kan være, og det er derfor referert til den diskursen i media som først og fremst går på *cyberterrorisme*. Siden begrepene går over i hverandre har det likevel vært nødvendig å ta med eksempler på mediediskursen rundt relaterte begreper. For å finne artikler er det foretatt grundige søk på Internett i databasene til Aftenposten, Dagbladet, VG, Computerworld og IT-avisen i Norge, og ellers i basene til BBC News, CNN.com, The Christian Science MonitorThe Times, The New York Times, The Washington Post, The Independent, The Guardian, The International Herald Tribune. Enkelte nyhetsbaser har vist overraskende få funn ved søk etter ordet cyberterrorisme, men har flere treff på f.eks. informasjonskrigføring. Det er også mange av de samme artiklene og henvisning til de samme forskningsrapportene eller politiske dokumenter som går igjen i mediekilden. I tillegg har det vært mulig å finne artikler på Internett-sider som f.eks. "infowar.com", og på nettsider til forskningsinstitusjoner og universiteter, men

kildene jeg har funnet på disse sidene har stort sett vært av akademisk art og ikke mediarelatert.

3.5 Oppsummering

Det er brukt både primærkilder (fra det akademiske og politiske miljø) og sekundærkilder (fra media)i denne oppgaven. I den forbindelse er det viktig å påpeke at i diskursanalyse vil nettopp sekundærkildene også være primærkilder. Det er uansett viktig å ha et godt og variert utvalg kilder siden hovedanalysen er en diskursanalyse av et *begrep*. Yin vektlegger bruk av ulike typer kilder som datagrunnlag for å kunne vise til kildetriangulering (Yin 1994:91-92). Ved å bruke flere og forskjellige kilder får forskeren et bredere undersøkelsesgrunnlag samt at resultatene vil virke mer overbevisende og sikre. Jeg mener jeg tar for meg et bredt utvalg kilder, slik at dette kriteriet ved datainnsamling blir oppfylt. Ved å studere ulike typer kilder innen ulike miljø kan man følge med diskursen og se hvordan den forandrer seg i ulike fora og innen ulike typer materiale. Metoden som er valgt i denne oppgaven har sine begrensninger, men valget av teori, og forholdet mellom teori og metode underbygger påstanden om at metoden er egnet til oppgavens problemstilling.

4. Begrepsavklaring

Dette kapittelet består av en begrepsavklaring på begreper som er sentrale i diskursen rundt cyberterrorisme og er ment som bakgrunnsmateriale til den videre analysen. Dette er viktig for å klargjøre at alt som blir omtalt som *cyberterrorisme* ikke nødvendigvis er *terrorisme* per definisjon. Begrepsjungelen er stor og omfattende, og det er gjort forsøk på å sortere ut begrepene og forklare hva de innebærer ettersom de ofte blir blandet og brukt om hverandre.

Cyberterrorisme, informasjonskrigføring, nettkrig m.m. er begreper som kan relateres til hverandre, og det ligger vanskeligheter i å skille dem. Det er ingen stringent analytisk forskjell mellom flere av begrepene, men man kan si at alle dreier seg om informasjon i en eller annen form. De futuristiske forskerne Heidi og Alvin Toffler forfekter ideen om at blant annet territorium blir mindre viktig og at informasjon blir hovedkilde til rikdom og makt i framtida. De hevder at kriger ikke lenger vil bli utkjempet for å tilegne seg territorium eller industrielle ressurser – i stedet vil ”the object of conflict” bli den nye strategiske verdien: *informasjon* (Toffler & Toffler 1993; Shapiro 1999). Allerede tidlig på 1980-tallet ga ”the Tofflers” ut bøker med futuristiske perspektiver og snakket om en informasjonsrevolusjon lenge før det ble vanlig å bruke Internett i dagliglivet. Grensene mellom begrepene er vage, en e-post bombe kan betraktes som hacking av noen og cyberterrorisme av andre (Denning 2000). Når det gjelder forsøket på en begrepsavklaring nedenfor må det nevnes at det finnes ingen *etablerte* definisjoner på de begrepene som skal avklares. Det er referert til definisjoner som går igjen i litteraturen og som blir brukt av fremtredende forskere innen fagområdet, samt statlige departementers definisjoner.

4.1.1 Cyberspace

Bunker har skrevet en artikkel om framtidig ”romlig utstrekning” (*spatial extent*) av slagmarken og diskuterer tradisjonalistene og reformistenes syn på dette. Reformistene mener i økende grad at en ny dimensjon må tilskrives slagmarken; i

tillegg til tid og rom må et nytt begrep legges til, *cyberspace*. Dette legges til slik at Internett og terrorister kan medregnes ”within the spatial parameters of the advanced battlefield which has emerged” (Bunker 1999). Bunker refererer til to definisjoner av cyberspace som kommer fra The National Defense Panel sin rapport ”Transforming Defense”. Definisjonen er todelt: ”1. The Global Information Infrastructure. 2. That aspect of the area of conflict composed of the electromagnetic spectrum and non-human sending dimension in which stealt-masked forces either stage attacks or seek refuge from them.” Definisjonen av cyberspace kan enten bestå av hele den todelte definisjonen eller bestå av kun den første delen av definisjonen.

Cyberspace kalles i mange tilfeller den virtuelle verden (*the virtual world*) og er av Barry Collin definert som ”symbolic – true, false, binary, metphoric representations of information – that place in which computer programs function and data moves” (Collin 1997).

4.1.2 Terrorisme

Det finnes mange ulike definisjoner på terrorisme, og det kan synes som om man ikke blir enige om én allment akseptert definisjon. US Department of State bruker følgende definisjon: ”The term ”terrorism” means premeditated, politically, motivated violence perpetrated against noncombatant target by subnational groups or clandestine agents, usually intended to influence an audience” (Hoffman 1998:38). Denne definisjonen blir ofte sitert. En anerkjent studie av europeisk terrorisme bruker denne definisjonen: ”en kalkulert frambringelse av frykt for skade eller død hos en gruppe, frambragt av bruk eller trussel om bruk av vold” (Engene 1994:29). Denning (1999:68)[14] definerer terrorisme som ”the actual or threatened use of violence with the intention of intimidating or coercing societies or governments”. Terrorisme kan

[14] Dorothy Denning har vært professor i datateknologi ved Georgetown University i Washington D.C. og leder av ”The Science and Technology in International Affairs program”. Hun er en av de fremste og mest anerkjente forskerne innen feltet cyberterrorisme og jobber nå som professor ved Naval Postgraduate School.. Hun har skrevet flere bøker om blant annet informasjonskrigføring, kryptering og datasikkerhet og har gitt ut mange papers og artikler om cyberterrorisme, hacking og relaterte emner.

utføres av individer eller ikke-statlige grupper og har ofte politiske eller ideologiske motiver.

Bruken av ordet ”noncombatant target” i US Department of State sin definisjon som Hoffman (1998) viser til kan kommenteres litt nærmere. De subnasjonale gruppene regner gjerne motmålet (f.eks. staten, det militære) for kjempende (combatant) i stedet for ikke-kjempende (noncombatant), og et eksempel på det er IRA[15] vs staten. I andre tilfeller er det riktig å bruke ”noncombatant” overfor målet fordi terroristene angriper overraskende og plutselig og de som blir angrepet har ikke mulighet til å kjempe for seg eller i mot terroristene. Videre er det sentralt at aktørenes *politiske motivasjon* nevnes i definisjonen. Dette bør være et krav for at noe kan kalles terrorisme. Når man snakker om terrorisme må det legges til at man ser for seg flere en én aktør. Hendelser som innebærer hacking av én person mot f.eks. Pentagon kalles av enkelte for cyberterrorisme, men hvis man tar hensyn til de ovennevnte kommentarene om terrorisme kan man stille spørsmål ved om det er en terroristhandling.

4.1.3 Cyberterrorisme

Begrepet *cyberterrorisme* ble først brukt i det akademiske miljø. Denning (1999:69) skriver at det var Barry Collin som på 1980-tallet samkjørte begrepene *cyber* og *terrorisme* til å bli *cyberterrorisme* i et forsøk på å vise konvergensen mellom cyberspace og terrorisme. O’Brien & Nusbaum (2000:54) nevner også at begrepet ”cyberterrorisme” er tilskrevet Barry Collin. Selv skriver Collin i artikkelen ”The Future of Cyberterrorism” (1997) at han satte sammen begrepet for et tiår siden som et bevis på den teknologiske avhengigheten og svakhetene som var i ferd med å formes i vår ”New World disOrder”. Han nevner *ikke* om han skrev ned begrepet cyberterrorisme i et dokument som har blitt utgitt, og det har ikke vært mulig å oppdrive den eventuelle kilden. Teknologisk avhengighet ble tidlig forutsett, av blant andre August Bequai. Han skriver om ”high-tech revolusjonen” som drives av

[15] IRA: Irish Republican Army.

menneskelig intellekt og som byr på nye utfordringer som kan være uforståelige og dermed vanskelig å takle (Bequai 1987). Han ser for seg en framtid hvor samfunnet er avhengig av smarte maskiner og hvor faren for "technocrimes" er stor. "The advances in computer technology in the last several years have been so great, and security has trailed so far behind, that it is now almost child's play to steal electronically" (Bequai 1987:49). Han påpeker i konklusjonen at datarevolusjonen har skapt nye former for kriminalitet som blir utnyttet av hackere, terrorister og kriminelle, og vi må handle før det får alvorlige konsekvenser.

Denning (1999:69) skriver "in the 1980s Barry Collin coined the term *cyberterrorism* to refer to the convergence of cyberspace and terrorism". Videre viser hun til FBIs arbeidsdefinisjon[16]: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine groups." Denning (2000b) selv definerer hva cyberterrorisme er og hva det ikke er på følgende måte:

"It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious crimes against cirtical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."

Det er denne definisjonen som legges til grunn for analysen i de neste kapitlene hvor vi ser nærmere på om rapporterte cyberangrep er cyberterrorisme og når diskursen

---

[16] Arbeidsdefinisjon av Mark Pollitt som har vært spesialagent i FBI. Denne definisjonen finnes også i et paper skrevet av Pollitt i forbindelse med akademiske studier ved George Washington University, USA, kalt "Cyberterrorism – Fact or Fancy?", årstall ukjent. I flere andre kilder står denne definisjonen som FBIs definisjon på cyberterrorisme.

rundt begrepet drøftes. FBIs definisjon henviser ikke til ønske om å skape *frykt*, noe som ofte nevnes i ulike definisjoner av terrorisme. Det bør være likhet mellom bruken av begrepene cyberterrorisme og terrorisme. Denning tar imidlertid med aspektet om frykt. Det samme gjør Stark (1999) som inkluderer aktørenes hensikter med terrorhandlingen (her: skape frykt, angst og panikk i målgruppebefolkningen). Motiver for handlingen, særlig politiske, er også essensielt i en definisjon av cyberterrorisme i likhet med terrorisme, og det har FBIs definisjon derimot tatt til orde for. Stark nevner også politisk motivasjon i definisjonen sin, men han bruker i tillegg ord som cyberkrigføring i en definisjon som går på cyberterrorisme. Krigføring og terrorisme er imdiertid ikke det samme. Stark (1999)[17] definerer cyberterrorisme slik: ”Målbevisst eller truende bruk av politisk, sosiologisk, økonomisk eller religiøst motivert cyberkrigføring eller cybermålrettet vold, utført av en ikke-statlig eller statssponset gruppe med den hensikt å skape frykt, angst og panikk i målgruppebefolkningen og å ødelegge militære og sivile verdier” (min oversettelse).

Stark anser cyberterrorisme som ethvert angrep mot en informasjonsfunksjon uansett middel. Begrepet informasjonskrigføring omfatter et stort spektrum av aktiviteter, men man ser spesielt for seg et scenario hvor informasjonsterrorister, kun ved hjelp av mus og et tastatur, hacker seg inn på datasystemer og får fly til å kollidere og å styrte, energinettverk til å bryte sammen, og forgifter matforsyninger (Denning 1999: xiii). For at begrepet ”cyberterrorisme” skal ha en mening så bør det kunne skilles fra andre typer datamisbruk som datakriminalitet, informasjonskrigføring osv. Det har blitt mer vanlig blant terroristorganisasjoner å benytte seg av IT; det vises blant annet på den økte bruken av web-sider til å drive propaganda og pengeinnsamling. Det har vokst fram en gruppe terrorister som kan kalles ”cyberterrorister”, dvs. at de skiller seg fra tradisjonelle terrorister siden de ikke bruker fysisk terror, men heller engasjerer seg i

---

[17] Stark skrev, som *graduate assistant* ved Southwest Missouri State University, Department of Defense and Strategic Studies, USA, en avhandling om cyberterrorisme (se bibliografi). Han tok opp mange interessante aspekter som definisjonsspørsmål, potensielle angrepskilder, våpen og taktikk, motiver m.m. Det står ikke årstall på utgivelse av avhandlingen, men han referer til rapporter og deltakelse på forelesninger høsten 1998. Jeg har benyttet en Internett-utskrift fra 1999 og velger å referere til Stark som Stark (1999). Dette var den første kilden jeg fant som definerte og drøftet cyberterrorismebegrepet på grundig, analytisk vis.

angrep på informasjonssystemer/kilder (Furnell & Warren 1999:30). Disse cyberterroristene blir som regel delt inn i individer, stater, og sub-statlige grupper eller nettverk[18].

4.1.4 Cyberwar, netwar og cybotage

Arquilla og Ronfeldt ved RAND Corporation har etablert begrepene cyberwar og netwar, og det er i hovedsak disse forskerne andre refererer til når de skriver om disse begrepene[19]. De brukes som referansekilde, men det skal vise seg at selv de som introduserer begreper ikke er konsekvente i sine ordvalg. Arquilla og Ronfeldt introduserte begrepet "cyberwar" for å sette kunnskapsrelatert konflikt på militært nivå. "*Cyberwar* refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself" (Arquilla & Ronfeldt 1993). Med andre ord, cyberkrig er militære operasjoner utført i forhold til informasjonsrelaterte prinsipper. Nettkrig derimot henviser til at informasjonsrelaterte kamper ofte er assosiert med lav-intensitetskonflikt mellom ikke-statlige aktører, deriblant ikke-governmentale organisasjoner (NGO'er) (Denning 1999:72). I "Cyberwar is coming!" hevder Arquilla & Ronfeldt (1993) at nettkrig brukes om lavintensitetskonflikter mellom ikke-statlige aktører som terrorister, narkotikakarteller og svartebørsselgere som driver salg av masseødeleggelsesvåpen. Senere i artikkelen skriver de at nettkrig henviser til konflikt på høyt nivå: "*netwar* refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it" (Arquilla & Ronfeldt 1993). De bruker lavintensitetskonflikt og konflikt på høyt nivå om nettkrig, og det er ikke samsvar

---

[18] Nærmere diskusjon om disse aktørene i kap.5.

[19] Se f.eks. Denning (1999); Stark (1999).

mellom disse begrepene. Dette viser hvor vanskelig det kan være å avklare og definere begreper. I andre artikler av Arquilla m.fl. refererer begrepet nettkrig til en kommende konfliktform i samfunnet som involverer få tradisjonelle krigsmidler, men økende bruk av nettverksformede organisasjoner, strategier, doktriner og teknologi avstemt etter informasjonsalderen (Arquilla m.fl.1998: 47; Arquilla m.fl.1999:82). Dettee er mer i samsvar med det de skriver tidlig i "Cyberwar is coming!", og det er grunn til å anta at det er dette de først og fremst legger i ordet nettkrig. De er opptatt av nettverksorganisering og ser for seg at framtidige konflikter vil bli utkjempet av grupper som er organisert mer som nettverk enn som hierarkier.

Utviklingen innen terrorisme er forbundet med nettverksutviklingen hvor makt i større grad blir overført til ikke-statlige aktører som organiserer seg i multi-organisasjonsnettverk framfor til tradisjonelle, hierarkiske statlige aktører. Terroristene organiserer seg i transnasjonale internettede grupper og bruker i økende grad avansert teknologi. Nettverk har med andre ord stor betydning for terroristers kapabiliteter. Nettkrigsaktørene vil sannsynligvis være ikke-statlige aktører bestående av både sub-nasjonale og transnasjonale grupper. Aktørene har ikke sentralt lederskap eller hovedkvarter som kan bli siktet på og alle medlemmene følger en felles doktrine. Nettkrig kan bli ført mellom regjeringer i rivaliserende nasjonalstater, av regjeringer mot ulovlige grupper som terrorister, narkotikakarteller osv., og av politiske grupper mot regjeringen. Karakteristiske trekk ved nettkrig er at deltagerne ikke nødvendigvis er organisert langs militære eller byråkratiske hierarkiske linjer og at konflikten styres ved hjelp av tastatur og modem i stedet for konvensjonelle våpen. I følge Stark (1999) er dette karakteristikker som skiller nettkrig fra informasjonskrig, men som har visse likheter med cyberterrorisme. Nettkrig er likevel forskjellig fra cyberterrorisme fordi nettkrig i stor grad går ut på å bruke cyber-taktikk for å lage forstyrrelser. "These tactics are generally associated with temporary disruption while cyberterrorism may involve the complete physical reconfiguration of targeted facilities" (Stark 1999).

Man kan stille spørsmål ved om det er et reelt skille mellom cyberkrig og nettkrig. Begge dreier seg om informasjon og kommunikasjon og former for "kunnskapskrig".

Hovedforskjellen er ment å være at cyberkrig har en militær side, mens nettkrig i utgangspunktet er ikke-militær. I cyberkrig settes vanligvis formelle militære styrker opp mot hverandre, mens nettkrig sannsynligvis involverer ikke-statlige, paramilitære og irregulære styrker (hvor terrorisme kommer inn) (Arquilla m.fl. 1999:82). Enkelte dimensjoner ved nettkrig kan likevel føre til at den utvikler seg til militær krig. Arquilla og Ronfeldt mener at en rekke teknologiske og ikke-teknologiske våpen vil bli brukt i nettkrig som i cyberkrig, og nettkrig involverer også psykologiske operasjoner (psyops) og ”perception management”.

Arquilla m.fl. (1998:68) beskriver tre paradigmer som gir rom for nettkrig og mener alle disse kan føre til at ”cybotage” oppstår: ”terror as coercive diplomacy, terror as war, and terror as the harbinger of a ”new world”. De definerer begrepet ”cybotage” på følgende måte: “Acts of disruption and destruction against information infrastructures by terrorists who learn the skills of cyberterror, as well as by disaffected individuals with technical skills who are drawn into the terrorist milieu” (Arquilla m.fl.1998:71).

4.1.5 Informasjonskrigføring/Informasjonsoperasjoner

> *”We live in an age that is driven by information. Technological breakthroughs…are changing the face of war and how we prepare for war.”*
>
> - William Perry, Secretary of Defense[20]

I et foredrag for Forsvarets Overkommando[21] i 1998 hevdet Benedicte Gude at begrepet informasjonsoperasjoner har erstattet begrepet informasjonskrig (Gude 1998:avsnitt 3). Hun sier at informasjonskrig blir forbundet med krig og krigføring mens informasjonsoperasjoner kan gjennomføres i fred eller krise og er et mer nøytralt begrep. Litteraturen på området viser at informasjonsoperasjoner blir brukt

[20] Sitert i Molander m.fl. 1996:xi.

[21] Forsvarets Overkommando ble lagt ned i 2003 og erstattet med Forsvarsstaben.

stadig mer, men det er fortsatt mange forskere som bruker informasjonskrig, og særlig i media blir begrepet brukt til stadighet, noe som trolig skyldes at ordet informasjons*krigføring* har en mer sensasjonell effekt. På en konferanse om *Information Warfare Post Y2K* i Washington D.C. etter milenniumskiftet (Grunnan 2000) brukte foredragsholderne begrepene om hverandre, og det lot til at det ikke var fullstendig enighet om at informasjonsoperasjoner er det ordet som skal brukes. Det er imidlertid i ferd med overta som det dominerende begrepet siden det rommer mye mer enn informasjonskrigføring som har en sterk assosiasjon til *krig*. I flere norske dokumenter, eksempelvis rapporten fra Sårbarhetsutvalget (NOU 2000:24) blir informasjonsoperasjoner brukt framfor informasjonskrigføring. Begrepsvalget har mye å gjøre med hvilket fora det brukes i. Som nevnt ovenfor bruker media i mye større grad informasjonskrigføring på grunn av nyhetsverdien ved bruk av ord med *krig* i. Forsvaret baserer seg på NATOs definisjon av informasjonsoperasjoner som fremgår av MC 422 *NATO Information Operation* Policy:

”Tiltak iverksatt for å påvirke beslutningstakere til støtte for egne politiske og militære målsettinger. Tiltakene har til formål å påvirke andres informasjon, informasjonsbaserte prosesser, kommando- og kontrollsystemer (K2S) og informasjons- og kommunikasjonssystemer, mens vi utnytter og beskytter vår egen informasjons og våre egne tilsvarende systemer. Informasjonsoperasjoner utnytter grensesnittet mellom teknologiske nyvinninger og den mest kritiske faktor i ethvert aspekt ved krigføring – mennesket. Det finnes to kategorier av informasjonsoperasjoner: defensive og offensive, avhengig av hvilke tiltak som iverksettes.” (Forsvarets fellesoperative doktrine 2000:71)

Den militære anvendelsen av informasjonsoperasjoner tar utgangspunkt i kommando- og kontrollkrigføring og kan defineres som:

”Den integrerte bruk av alle militære kapasiteter, herunder operasjonssikkerhet (OPSEC), villedning, psykologiske operasjoner (PSYOPS), elektronisk krigføring (EK) og fysisk ødeleggelse for å påvirke, svekke, ødelegge eller nekte informasjon til en motstanders kommando- og kontrollsystem, og for å beskytte vårt eget mot tilsvarende virksomhet.” (Forsvarets fellesoperative doktrine 2000:72)

Informasjonsoperasjoner på strategisk nivå kan inneholde både militære og sivile tiltak, mens C2W er en ren militær strategi som kan plasseres på et operasjonelt nivå.

NATOs definisjon antyder at informasjonsoperasjoner kan være både offensive og defensive. Offensive operasjoner brukes for å få tilgang på informasjon og datasystemer og kan omfatte elektronisk krigføring, jamming, villedning, psyops m.m. Defensive operasjoner har først og fremst til hensikt å forhindre eller redusere mulighetene for offensive operasjoner mot ens egne systemer og virkemidler her er brannmurer, kryptering, backup systemer m.m. (Gude 1998: avsnitt 3.1; O'Brien 2000).

O'Brien (2000:1) viser til ulike definisjoner på informasjonsoperasjoner (IO). Det amerikanske forsvarsdepartementet snakker om "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information." Det britiske forsvarsdepartementet snakker om "deliberate…and systematic attack on critical information activities which seeks to exploit, modify, corrupt information and deny service." US *Joint Publications 3-13 (Joint Doctrine for Information Operations)* definerer IO som: "actions taken to affect adversary information systems while defending one's own information and information systems… IO capitalises on the growing sophistication, connectivity, and reliance on information technology. IO targets information or information systems in orderr to affect the information-based process, whether human or automated" (O'Brien 2000:2). Videre viser O'Brien til at man kan skille ut tre nivåer av informasjonsoperasjoner. På det høyeste nivået oppfattes IO som "an ideational struggle for the mind of an opponent", på det andre nivået blir IO ofte sidestilt med "Revolution in Military Affairs (RMA)", og på det laveste nivået består IO av angrep på og forsvar av informasjonsflyt og aktiviteter (O'Brien 2000:3).

Arquilla m fl. (1999) forsøker å definere informasjonskrigføring i forbindelse med forholdet mellom *just war* teorien og informasjonskrigføring. Siden begrepet

informasjonskrigføring ble introdusert har det utviklet seg og inkluderer i dag mange aktiviteter som er informasjonsrelatert, men som ikke betraktes som krigføring. Arquilla velger å dele opp begrepet og sier det slik at *informasjonsoperasjoner* refererer til informasjonsintensive samhandlinger på tvers av et spektrum som inkluderer psykologiske operasjoner, ”perception management”, informasjonssikkerhet og informasjonskrigføring. Siden informasjonsoperasjoner også brukes er det mulig å ”reservere” begrepet informasjonskrigføring for bestemte former for krigsaktiviteter. Informasjonskrigføring er dermed en type krig som har som mål å treffe kommunikasjonsnoder og infrastrukturer (Arquilla 1999b:384). I slike angrep slår man til via cyberspace og bruker ”våpen” som logiske bomber og datavirus, men det er også mulig å bruke andre offensive midler som konvensjonelle våpen.

Stark (1999) mener at den viktigste forskjellen mellom cyberterrorisme og informasjonskrigføring ligger i *hvem* angriperen er. Hvis en *stat* står bak angrepet blir det betraktet som informasjonskrigføring, og dersom angrepet blir utført av en terroristgruppe *eller* en annen sub-nasjonal enhet er det cyberterrorisme. I følge USAs Department of Defense er cyberkrig og fysisk ødeleggelse av cybermål klassifisert som informasjonskrigføring hvis angriperen er en stat i stedet for en statssponset aktør eller en individuell aktør. Både cyberterrorisme og informasjonskrigføring er midler som brukes for å ødelegge informasjonssystemer til en motstander. Cyberterroristangrep kan være isolerte eller spontane, mens informasjonskrigføring vil sannsynligvis være en ”støtte” til militære operasjoner eller kampanjer (Stark 1999).

Informasjonskrigføring blir også omtalt som å ødelegge informasjon, redusere informasjonsflyt, redusere troverdigheten i informasjonsinnhold og nekte tilgang til tjenester (Devost 1995:14). Informasjonskrigføring kan føres mot industri, politiske innflytelsessfærer, globale økonomiske krefter og mot stater. Devost (1995) ser på informasjonskrigføring både i en politisk kontekst og som terrorisme. I rammen av en politisk kontekst ser han på hvordan stater skal takle trusler på

informasjonskrigføring, hvilke strategiske fordeler man får med å føre informasjonskrigføring osv. Som terroristverktøy er informasjonskrigføring veldig attraktivt, men mange terrorister vil kanskje føle at et informasjonskrigføringsangrep ikke skaper nok frykt og vil fortsatt mene at tradisjonelle bomber er mer effektive. Informasjonskrigføring vil trolig bli brukt sammen med konvensjonell krigføring. Stark er opptatt av skillet mellom stat og individuell aktør når det gjelder forholdet mellom cyberterrorisme og informasjonskrigføring. Devost derimot nevner både stater, grupper og individuelle personer som mulige aktører som kan føre informasjonskrigføring. Han nevner blant annet eksempler på en britisk hacker som infiltrerte det amerikanske Forsvarsdepartementets datasystem i sju måneder og kaller dette informasjonskrigføring (Devost 1995:25). Hvis man skal følge Starks definisjoner og begrepsavklaringer ville dette blitt kalt cyberterrorisme fordi det er en individuell person som er angriperen, men det ville derimot ikke vært et eksempel på cyberterrorisme i følge Dennings definisjon (Denning 2000b). Analysen vil vise om det politiske og akademiske miljø sine vanskeligheter med å bli enige om en felles definisjon kan påvirke i hvilken grad cyberterrorisme er sikkerhetisert.

Avslutningsvis kan det nevnes at strategisk informasjonskrigføring også er et begrep som har blitt mye brukt i forbindelse med informasjonskrigføring. Informasjonskrigføring er et begrep som er og har vært i rask utvikling og er et nytt interessefelt for forskere, militære og andre beslutningstakere. Molander m.fl. (1996) skriver at det amerikanske militæret må reagere raskt for å dra nytte av nyvinningene innen informasjonsteknologi. Samtidig fører den teknologiske utviklingen til at USA får nye motstandere som vil forsøke å utnytte den voksende globale informasjonsinfrastrukturen til militære formål. Informasjonskrigføring har ofte blitt sammenlignet og/eller likestilt med kommando- og kontrollkrigføring (C2W) og elektronisk krigføring (E2). Nå blir begrepet i økende grad brukt som en samlebetegnelse for ulike krigføringskonsepter forbundet med *Informasjonsalderen*. Informasjonskrigføring har en generell betydning i vanlig bruk i og med at man ikke har kommet fram til en enstemmig definisjon av begrepet. I følge Molander m.fl. (1996:1) er det et element som er i ferd med å dukke fram i informasjonskrigføring

som krever en definisjon; det at nasjoner bruker cyberspace for å påvirke strategiske militære operasjoner og påfører nasjonale informasjonsinfrastrukturer skader blir kalt ”strategisk informasjonskrigføring”.

5. Oppbygging av et potensielt trusselbilde

"Cyberattacks are now likely to be within the capabilities of a number of terrorist groups."[22]

Det foregående kapittel med begrepsavklaringer var ment som bakgrunn for å prøve å vise om bildet av en mulig trussel, cyberterrorisme, har blitt generert til å utgjøre en sikkerhetstrussel. For å løse dette vil to faktorer studeres i dette kapittelet: Talehandlinger som går på trusselvurderinger gjort av de sikkerhetiserende aktørene, forskere og politikere (5.1), samt analyse av empiriske eksempler som bygger opp om et potensielt trusselbilde (5.2). Vi lever i et sårbart samfunn som følge av teknologisk utvikling, og det er av en slik karakter at det kan rammes av farene som beskrives i trusselvurderingene. Ved å studere "speech acts" om hvilke aktører som utgjør en trussel, hvilke midler de disponerer, hvilke mål de kan tenkes å rette angrep mot (hvilke sentrale verdier som er truet), og hvilke hensikter de måtte ha, samt ved å liste opp en rekke empiriske eksempler på cyberangrep, vil man kunne få et innblikk i hvilket bilde av en mulig sikkerhetstrussel som har blitt dannet. Som nevnt tidligere er det paradoks at det ikke finnes registrerte cyberangrep som kan settes i kategorien *cyberterrorisme* i henhold til definisjonen jeg holder meg til (jfr. masseødeleggelse). Det faktum at det ikke finnes eksempler på rene cyberterroristangrep er nevnt av flere forskere, blant annet Denning (1999), og det blir sentralt å prøve finne eksempler på ulike cyberangrep som jeg mener kan bekrefte eller avkrefte dette. Derfor har jeg et avsnitt med empiriske eksempler på ulike cyberangrep, utført av ulike trusselaktørgrupper i dette kapittelet.

---

[22] CSIS 1998: 29. Sitat av John Deutch, direktør i CIA 1995- 96.

5.1 Hvorfor har bildet av en mulig trussel blitt generert?

5.1.1 Et sårbart samfunn

De mest sentrale effektene av globaliseringen er at den bipolære verden er forsvunnet etter den kalde krigen og at teknologien er forbedret slik at kommunikasjons-mulighetene er mye større for et globalt publikum. En utvikling er på gang mot økt bruk av desentraliserte styringsstrukturer framfor hierarkiske. Flytende allianser, ad hoc-koalisjoner og *nettverk* dannes mellom grupper og individer. Et mulig resultat av dette er at grupper av amatører og profesjonelle terrorister samarbeider for én bestemt sak og løses opp etterpå. En ny trend i samfunnet er at vi går mot økende individualisme og personifisering. Følelsen av at vi lever i et globalt samfunn har også endret lojalitetsfølelsen. Innenfor ulike miljøer føler man stor tilhørighet til den internasjonale gruppa man er en del av (f.eks. innen hackermiljøet hvor det finnes mange cybergrupper med global rekkevidde).

Kritisk infrastruktur er i teorikapittelet omtalt som oppgavens *referanseobjekt* (en sentral verdi som er truet), og blir som regel definert som telekommunikasjon, elektrisk kraftforsyning, gass- og oljeaktiviteter, bank og finans, transport og ferdselsårer, vannforsyning og nødhjelpssystemer (helse, politi, brann). I dagens globale samfunn må sivil infrastruktur og dens beslutningstakere også regnes som utsatte mål i tillegg til de tradisjonelle militære. Skader på infrastrukturen vil få store konsekvenser for innbyggerne. Det er imidlertid stor usikkerhet knyttet til om terrorgrupper kommer til å gjennomføre aksjoner i cyberspace i stedet for med de tradisjonelle virkemidlene, og det er ingen terrorgrupper som har gjennomført alvorlige terrorangrep mot informasjonssystemer som styrer kritisk infrastruktur (Lia 2000:17).

Allerede eksisterende terroristvirksomhet blir gjort enklere ved hjelp av den nye teknologien. Den virkelige trusselen i en ”cyber” kontekst er når Internett blir medium for et terroristangrep. Internett var ment som et middel for å sikre fortsatt kommunikasjon i tilfelle en atomkrig ville ødelegge den konvensjonelle

telekommunikasjonsinfrastrukturen, men er i dag et medium som selv kan brukes til å gjøre skade på det nye informasjonssamfunnet (Furnell & Warren 1999:31). Informasjonsoperasjoner er ikke noe nytt. Bruk av informasjon i krig er like gammelt som krigføring i seg selv. Det kan ikke betraktes som nytt å påvirke en motstander ved hjelp av informasjon. Det er den teknologiske utvikling og de muligheter den har gitt oss som er ny og som kan utgjøre en trussel for oss. Både forskere, politikere og journalister later til å være enige om at utviklingen av den globale informasjonsinfrastrukturen har gjort høy-teknologilandene svært avhengige av IT og samtidig gjort dem sårbare overfor trusler som har oppstått i kjølvannet av dette. Globale informasjonsnettverk blir sett på som inngangsporter for stater, grupper og organisasjoner som av politiske og kriminelle årsaker ønsker å ramme f.eks. en annen stat. Via disse nettverkene er det mulig å overføre datavirus og bruke andre hacking-metoder for å ødelegge sentrale verdier som kritisk infrastruktur, som igjen vil påvirke befolkningen på mange måter, blant annet økonomisk.

En følge av informasjonssamfunnets sårbarhet er at det blir utsatt for ulike trusler og kan rammes av alvorlige virkemidler som de truende gruppene innehar. I de neste avsnitt ser vi nærmere på hvilke aktører som framstilles som truende, hvilke virkemidler de kan tenkes å bruke, samt hvilke mål og hensikter trusselaktørene kan inneha. Drøftingen tar utgangspunkt i figuren nedenfor[23].Figuren viser hva som ofte siteres som trusler, midler, mål, og hensikter og avhengigheten mellom punktene i hver av de fire kategoriene kan gå på kryss og tvers. Avhengighetskjeden trussel-middel-mål-hensikt kan f.eks. være *stat-økonomisk angrep-bank og finans-økonomisk fordel*, eller f.eks. *stat/informasjonskrigføringsgruppe-cyberangrep-kritisk infrastruktur-sikkerhetsfordel* (Flynt 2000:20).

---

[23] Figuren er hentet fra Bill Flynt (2000):"Threat Kingdom", *Military Review* July- August. Hans artikkel er basert på en analyse av en publikasjon av to kinesiske offiserer: Qiao Liang & Wang Xiangsui (1999): *Unrestricted Warfare*, oversatt. Foreign Broadcast Information Service. Beijing: PLA Literature and Arts Publishing House.

Figur 2: Trusler, midler, mål, hensikt

Trusler	Midler	Mål	Hensikt
Autonom terroristgruppe	Cyberangrep	Bank og finans	Sikkerhetsfordel
Informasjonskrigføringsgruppe	Informasjonsoperasjoner	Business	Økonomisk fordel
Stat	Økonomiske angrep	Befolkning	Finansiell gevinst
Hackere	Bombing	Kritisk infrastruktur	Politisk påvirkning
Statssponset terrorisme	Direkte handling	Kritisk infrastruktur	Politisk endring

5.1.2 Trusler

Trusler rettet mot kritiske infrastrukturer deles gjerne i to kategorier: fysiske trusler og cybertrusler. Fysiske trusler er knyttet til angrep på håndgripelig eiendom, mens cybertrusler er trusler fra elektroniske angrep rettet mot informasjons- eller kommunikasjonskomponenter som kontrollerer kritisk infrastruktur. Cybertrusler blir som regel definert som e-post virus, ormer, hacking, denial of service, uautorisert adgang til kontrollsystemer og nettverk osv. I figur 1 (se 2.3) som er en modell for hvordan man kan undersøke om cyberterrorisme har blitt sikkerhetisert defineres truslene nettopp som midler som hacking, denial of service osv. I annen litteratur, og som vi ser i figur 2, refereres ofte trusselen til aktører (grupper) som kan tenkes å ha midler og hensikter til å ramme sine utvalgte mål. Det er denne typen trusler vi skal se nærmere på i dette kapittelet. Tidligere så man kanskje på ulike innbrudd i og ødeleggelse av datasystemer som cybertrusler, men etter hvert har man i større grad begynt å se på hvilke ondsinnede aktører som har hensikter, motivasjon og ressurser til å gjennomføre slike angrep, og aktørene blir dermed sett på som en del av truslene også. Erfaringene fra denne drøftingen tas med til det neste analysekapittelet hvor vi ser nærmere på diskursen rundt begrepet cyberterrorisme i ulike kontekster. Når vi snakker om *aktører* i dette kapittelet henvises det til med andre ord til trusselaktører, ikke sikkerhetiserende aktører.

Fram til nå har vi ikke sett at terrorgrupper har gjennomført alvorlige terrorangrep mot informasjonssystemer som styrer kritisk infrastruktur. Man bør være forsiktig med å rette fokus mot politiske terrorister som de mest sannsynlige aktører. Aktørgruppen utgjør en svært sammensatt gruppe. Samfunnet (i form av sivile og militære systemer) kan bli utsatt for trusler fra ulike aktører som hackere, terroristorganisasjoner, stater, organiserte kriminelle grupper, industrispioner, misfornøyde ansatte i bedrifter (”insidere”), miljø- og dyrevernaktivister og nasjonale etterretningstjenester.

Fra slutten av 1990-tallet har flere og flere terroristorganisasjoner, selv de som er små, begynt å bruke Internett for å drive propaganda for sin virksomhet. I juni 1998 meldte *U.S. News & World Report* at 12 av de 30 gruppene som står på Det amerikanske utenriksdepartementets liste over terroristorganisasjoner er på Web’en (Denning 1999:68). Når terroristgrupper først får etablert seg på nettet er det vanskelig å fjerne dem fordi de kan drive hjemmesiden fra land med tale- og pressefrihet som ikke forbyr denne type virksomhet. Lia (2007) skriver at til tross for interne diskusjoner om Internett-aktivisme var kompatibelt med islamistiske trossetninger og doktriner på midten av 1990-tallet, ble etter hvert radikale islamister, eller ”jihadi”-grupper godt etablert på World Wide Web. Internett har blitt et stadig viktigere verktøy for disse gruppene i løpet av de siste ti årene, også for al-Qaida. ”It seems clear that the primary purpose of al-Qaida’s exploitation of the Internet is in the domain of propaganda and proselytising” (Lia 2007).

Cyberterrorisme antas å bli mer attraktivt for terroristgrupper fordi angrepene kan være anonyme og det blir vanskelig å finne gjerningsmennene, man kan leie hackere for å få nødvendig ekspertise, det er mulig å tiltrekke seg støttespillere fra hele verden, et vellykket angrep vil bli rapportert over hele verden, Internett er et ideelt propaganda- og pengeinnsamlingsredskap, og man kan skape store finansielle ødeleggelser uten at liv går tapt (Furnell & Warren 1999:33). Stadig flere stater begynner å ta truslene på alvor og danner forskningssentre- og programmer som har som mål å utrede sårbarhetene og øke sikkerheten (Grunnan 2000).

Arquilla m.fl. (1999) snakker om en fremvekst av en såkalt ”ny terrorisme” i forbindelse med utviklingen av informasjonsalderen. De mener terrorismen som er i utvikling kan kalles *nettkrig* fordi nøkkelen til å bekjempe terrorisme i informasjonsalderen er å bruke nettverk for å bekjempe nettverk. Ved økt bruk av nettverk flytter makten seg til flere ikke-statlige aktører ettersom de danner transnasjonale internettede grupper med desentralisert struktur, framfor den tradisjonelle organisasjonsformen med hierarkisk struktur dominert av statlige aktører. Arquilla m.fl. (1999) ser for seg at truslene i informasjonsalderen blir mer diffuse og multidimensjonale og at *cyberkrig* og *nettkrig* vil dominere konfliktmønsteret. Nettkrigsbegrepet passer inn med mønstre og trender som sees i Midtøsten hvor nye terroristgrupper ser ut til å ha desentraliserte, fleksible nettverksstrukturer (Arquilla m.fl. 1998:57).

Nedenfor ser vi nærmere på en rekke aktører vi kan bli utsatt for trusler fra.

5.1.2.1 Autonome terroristgrupper

Sub-statlige grupper kan være alt fra opposisjonsbevegelser, organiserte paramilitære til terroristorganisasjoner. *Autonome terroristgrupper* blir definert som en gruppe som har politiske mål og motiver, som er voldelig, som fører operasjoner med vidtrekkende psykologiske effekter langt utover hovedofferet eller målet, som har en identifiserbar kommandokjede (hvor medlemmene ikke bærer uniform), og som er en sub-nasjonal gruppe eller ikke-statlig enhet (Hoffman 1998:43, Flynt 2000:18). Tradisjonell terrorisme er basert på historie, kultur, religion m.m., mens cybertrusselen vil komme fra desentraliserte grupper med etnisk mangfoldighet som driver med kommunikasjonskapring og sosiale revolusjoner (Rodal 2000:12). Terroristgrupper kan benytte seg av informasjonsvåpen for å gjennomføre propagandakampanjer, drive pengeinnsamling, og for å angripe nasjonal infrastruktur. De fleste eksempler på bruk av informasjonsvåpen av terrorister faller inn under den første kategorien, som f.eks. portugisiske hackeres modifisering av web-sidene til det indonesiske utenriksdepartementet, hackere som har gjort om CIAs web-side til ”Central Stupidity Agency” osv. (Rathmell m.fl.1997: avsnitt 3.1). Rathmell m.fl.

bruker en rekke slike eksempler for å anslå at potensialet for terroristaktiviteter for å få publisitet er enorm, men utfordringen ligger i å overtale hackere til å jobbe for dem eller videreutvikle sitt eget kunnskapsnivå. Cyberspace danner en ny arena som terrorister og politiske ekstremister kan operere i. Islamistiske grupperinger har benyttet seg av den økte muligheten til å ha økt forbindelse med hverandre, noe som informasjons- og kommunikasjons-teknologien har gjort mulig (Whine 1999:123). Cyberspace vil trolig bli mer og mer attraktivt som forum for propgandavirksomhet, kommunikasjon, opplæring osv. innenfor terroristnettverk- og grupperinger, samt en arena hvor terroristhandlinger kan utføres.

5.1.2.2 Statlige aktører

Trusselen for cyberangrep fra *statlige aktører* mot samfunnsvitale informasjonssystemer anses som liten i fredstid, men desto høyere i krisesituasjoner. Det er kjent at flere stater arbeider konkret med å utvikle nasjonale strategier for bruk av angrep mot infrastruktur som middel mot en annen stat. Kina har offentlig gått ut og meddelt at de er åpne for å bruke informasjonskrigføring, og i henhold til bøker og avisartikler jobber kineserne aktivt med å videreutvikle sine informasjons-teknologiske kapasiteter for bruk i krigføring (Grunnan 2000:16). To kinesiske generaler har gitt ut en bok "Krig uten grenser" hvor de skriver at Kina bør ta i bruk terrorisme, datavirus og miljøskader i krig mot Vesten (Viken 1999). Hvor stor makt disse generalene har og hvordan kineserne har reagert på denne utgivelsen vet vi ikke noe om, men det er likevel en interessant observasjon om hvilket scenario framtida kan by på[24]. USA har også bygget opp en betydelig kapasitet på området, og Russland er i ferd med å utvikle spesielt sine teknologiske kapabiliteter og har allerede kommet langt på forskning innen psykologisk forskning og krigføring (Grunnan 2000:15). Andre stater som kan være potensielle cyberterrorister er Iran, Irak og Libya som har begynt å inkludere informasjonskrigføring i sin militære doktrine. Disse landene kan *forventes* å bruke cyberterrorisme (sannsynligvis gjennom sine egne statssponsete

[24] Det er som nevnt ovenfor analyse av denne boka figur 2 er basert på.

terroristgrupper) som et middel til å fullføre planer på den nasjonale agenda i skyggen av anonymitet (Stark 1999.). Stater som India og Pakistan har også drevet med ”cyber-kampanjer” mot hverandre, spesielt i form av hacking av statlige internettsider. Foruten stater med cyberkunnskap finnes en god del uavhengige aktører som videreutvikler sin kapasitet til å sette i gang informasjonskrigføring ved å stjele teknologi fra andre land ved hjelp av cyberspionasje.

5.1.2.3 Hackere

”Hackere brukes om folk med nok teknisk innsikt til å kunne manipulere datamaskiner og telekommunikasjonssystemer, og som spesielt forsøker å bryte seg gjennom andres sikkerhetssystemer” (Rodal 2001 [samtaler]). Det finnes etter hvert flere og flere profesjonelle hackere som tilbyr tjenestene sine på det åpne marked, og denne gruppen kan tenkes å utnyttes av sub-statlige grupper i stadig større grad. Når det gjelder amatørhackerne hacker mange av dem for moro skyld bare for å se hvilke systemer de greier å komme seg inn på og for å teste og utvikle sine egne datakunnskaper. Hackermiljøet er preget av mye spenning og prestisje, og hackerne prøver til stadighet å skape nye utfordringer for seg selv og andre. Som en følge av dette vil det være en del hackere som har tilsiktede hensikter og hacker for bevisst å ødelegge eller ramme noen, og dermed oppnå f.eks. større prestisje i miljøet.

5.1.2.4 Statssponset terroristgruppe

Statssponsede terroristgrupper er grupper som har samme kjennetegn som de autonome, men som mottar støtte til logistikk, trening, etterretning o.l. fra en stat og utfører angrep i overensstemmelse med operasjonell veiledning fra den staten (Flynt 2000:18).

5.1.2.5 Kriminelle grupper

Kriminelle grupper har aktivt begynt å bruke informasjonsteknologi til kommunikasjon og spede angrep på datasystemer. Trusselen mot norske interesser har hittil ikke vært stor, men i følge en trusselvurdering fra Økokrim antas flere grupper å

være en trussel for norsk næringsliv de kommende årene (Rodal 2001 [samtaler]). Kriminelle leier inn personer med store datakunnskaper for å utføre oppdrag for dem, og både overvåkingspolitiet og den militære etterretningstjenesten har flere eksempler på at folk er brukt eller misbrukt til å begå ulike lovbrudd.

5.1.2.6 Ansatte i bedrifter ("Insidere")

Cybertrusselen fra ansatte i bedrifter ("*insidere*") må ikke undervurderes. Det er lett å tro at den største trusselen kommer fra utenforstående hackere fordi de antas å ha de tekniske ferdighetene som kreves, men trusselen kan også komme innenfra. En misfornøyd ansatt kan ønske å hevne seg og utnytter sin posisjon. En amerikansk undersøkelse viser at 85 % av datainntrengningene begås av nåværende eller tidligere ansatte. I mange tilfeller utgjør hackerne utenfra en mindre trussel enn de innenfor fordi både ansatte, konsulenter og leverandører kan ha tilgang på bedriftens nettverk (Rodal 2001 [samtaler]). Cyberangrep og datakriminalitet fra "insidere" antas å øke i framtida, og Norge kan ikke regne med å "slippe unna". Det finnes allerede eksempler på utro tjenere i Norge, og Økokrim har engasjert seg sterkt i å forhindre økt datakriminalitet. I 2003 ble Politiets datakrimsenter åpnet og organisert under Økokrim[25].

5.1.3 Midler

Teknologiutviklingen har ført til en revolusjon på sivilt utviklet teknologi samt at militær teknologi er i rask utvikling (spesielt USA driver omfattende programmer innen militærteknologi). Nye typer midler/verktøy/våpen kan brukes til å gjennomføre mer eller mindre "uskyldige" angrep samt større angrep av alvorlig karakter. Begrepet "informasjonsvåpen" har ennå ikke blitt eksakt definert (Krutskikh 1999:30), men kan forklares som midler og metoder brukt for å skade andre staters informasjonsressurser (Tsygichko 1999). Det er mulig å klassifisere informasjonsvåpen basert på tenkt bruk

[25] Datakrimsenteret ble overført til Nye Kripos i 2005.

og funksjon. Informasjonsvåpen kan ha en militær funksjon eller de kan brukes for å knytte sammen data- og telekommunikasjonssystemer og nettverk (ibid.). Virus, "trojanske hester", elektromagnetiske pulsvåpen er eksempler på nye informasjonsverktøy dagens aktører har mulighet til å benytte.

Som følge av den teknologiske utviklingen kan sårbare samfunn rammes av harde og myke (fysiske og ikke-fysiske) virkemidler som kan gi store skadevirkninger. Som myke virkemidler regnes gjerne hacking og bruk av virus, logiske bomber, trojanske hester m.m. Dette er virkemidler som brukes til å påvirke, ødelegge, degradere eller misbruke kritisk informasjon eller de samfunnsvitale informasjons- og kommunikasjonssystemer som denne informasjonen er avhengig av. Angrep med bruk av disse virkemidlene kalles cyberangrep, men aktørene har også flere midler de kan bruke for å nå sine mål og oppnå sine hensikter. Foruten cyberangrep er informasjonsoperasjoner, økonomiske angrep, bombing og/eller annen direkte handling, midler som kan benyttes, jf. figur 2.

5.1.3.1 Cyberangrep

Cyberangrep[26] er angrep mot datanettverk fra, gjennom og mot datasystemer for å kontrollere, nekte, endre eller ødelegge systemets funksjoner. Slike angrep regner man med kan rettes mot kritiske infrastruktur som er styrt av datateknologi. Det finnes mange ulike måter å oppnå kontroll over data-, informasjons- og kommunikasjonssystemer på. *Sniffing* er en teknikk som brukes til å fange opp passord ved å lytte på nettverkstrafikken. *Spoofing* innebærer å utgi seg for noen man ikke er ved f.eks. å bytte ut IP-adressen. *Trojanske hester* er et program som bygges inn i og skjules i et annet program og som utfører en "forkledd" funksjon. Dette er et skjult program (bakdør) som kan bygges inn i vedlegg til moro-mailer, som diverse filmsnutter, og installeres under kjøring. Det er en populær metode for å legge inn skjulte virus og ormer. Etter installeringen kan avsender også komme seg inn i

[26] Cyberangrep er brukt som begrep i figur 2, derfor brukes ikke begrepet cyberterroristangrep her.

maskinen og ha full kontroll over den. Den trojanske hesten fungerer da som en bakdør som angriperen kan benytte for å få tilgang til maskinen. Trojanske hester kan også legges inn i programmer som selges på markedet. *Datavirus* kopierer seg selv i et større gram slik at programmet blir modifisert, og det begynner bare å virke når "vertsprogrammet" begynner å gå. Virus kan reprodusere seg selv og sprer viruset videre ettersom det reproduseres. En *orm* er et uavhengig program som reproduseres ved å kopiere seg selv fra en datamaskin til en annen over et nettverk. Elektronisk *jamming* blir brukt til å blokkere kommunikasjonskanaler på motstanderens utstyr slik at det blir umulig å motta informasjon. I stedet for å blokkere kan man også overøse systemet med ukorrekt informasjon for nettopp å desinformere. Under et *denial of service*-angrep (DoS) prøver angriperen å "mette" datamaskinen med så mye informasjon at den overbelastes. Dette forårsaker tjenesteavbrudd og setter målmaskinen ute av stand til å utføre sine vanlige oppgaver.

5.1.3.2 Andre midler

Informasjonsoperasjoner er beskrevet i punkt 4.1.5, men går i hovedsak ut på at man utfører handlinger som skal påvirke motstanderens informasjonssystemer samtidig med at man forsvarer sine egne informasjonssystemer. Cyberangrepsmidlene kan også brukes i informasjonsoperasjoner, ofte som del av en større kampanje eller krigføring. *Økonomiske angrep* er nevnt som et middel i figur 2 og med dette menes angrep på en motstanders økonomiske interesser via handelssanksjoner, frysing av finansielle verdier, varedumping, destabilisering av valuta m.m. (Flynt 2000:18). Middelet *bombing* innebærer bruk av ukonvensjonelle bomber, og *direkte handling* viser til et fysisk angrep rettet direkte mot et mål, det være seg av uniformerte væpnede styrker, terrorist- eller geriljastyrker (ibid.)

5.1.4 Mål

Aktørene som regnes som en trussel for samfunnet kan ha forskjellige mål for sine handlinger, fra å ramme befolkningen direkte gjennom bombeangrep på bygninger til angrep på kritisk infrastruktur som kraftforsyning ved hjelp av hacking. I følge

framstillingen til Flynt i figur 2 blir kritisk infrastruktur, befolkning og business som regel sett på som de mest sannsynlige målene for ulike typer angrep av ulike typer aktører. I figur 1 i kapittel 2 har jeg også satt opp kritisk infrastruktur som referanseobjekt (sentral verdi som blir truet). Det antas at hackere vil ha business og kritisk infrastruktur (kanskje særlig bank og finans, men også tele- og kraftforsyning) som et viktig mål, mens terrorister tradisjonelt har rettet aksjoner mot befolkningen i form av bombing av symbolske mål som ambassader, banker osv., og den senere tid aksjoner på spesielt offentlige transportmidler. Det skrives svært mye om faren og trusselen for at terrorister vil begynne å rette angrep mot infrastruktur. Eksemplene som beskrives nedenfor gir et bilde på hvilke mål som ser ut til å være de viktigste og hvem det er som har det som mål. Den videre analysen kan gi et bilde på hvordan forskere, politikere og journalister ytrer seg angående muligheten for samfunnsvitale infrastrukturer som mål for angrep.

5.1.5 Hensikter

Noe av det vanskeligste man kan studere er *intensjonene* til forskjellige grupper, men det er gjort flere forsøk på å anta hvilke hensikter de har hatt eller kan ha. Når det gjelder utviklingen av informasjonsteknologi og utnyttelsen av denne hevdet Hoffman (2000) [27] at terrorister benytter seg av IT først og fremst for egen ervervelse framfor å ødelegge. ”Terrorists are intelligence freaks”(ibid.). Det er hackerne som driver med det som gjerne kalles og oppfattes som cyberterrorisme, mens terroristene er ute etter å bruke IT av etterretningshensyn og propaganda. Hoffman påpeker at politisk radikale terrorister som regel er konservative i handlingsmønster (ibid.). Terrorisme i dag reflekterer store endringer og nye motstandere har oppstått, og amerikanerne mener at våpen og taktikk har *ikke* endret seg til tross for antakelser om det motsatte. De fleste terrorister holder seg til bruk av tradisjonelle bomber.

---

[27] Hoffmans uttalelser kom i forbindelse med en Workshop med TERRA-prosjektet ved FFI 26. september 2000 og innlegget ”New and Continuing Forms of Terrorism” på seminaret *Terrorism – Past, Present and Future* på Oslo Militære Samfund 27. september 2000 (se Lia & Andrésen 2000).

Flere forskere ved RAND[28] tror at terrorister vil hacke seg inn på datasystemer, men hovedsakelig for å samle informasjon for å gjennomføre aksjoner. I mange tilfeller vil det være vel så effektivt for terroristene å bryte seg inn i data- og sikkerhetssystemer for å få tak i informasjon om nøkkelpersoner og deretter ramme *dem* direkte. IRA har f.eks. hacket seg inn på statlige kjøretøyregistre i Storbritannia for å skaffe informasjon, ikke for å ødelegge kjøretøysregisteret og slik skape kaos. Hoffman (2000) mener at det er slike tilfeller vi vil få se mer av. Terroristene vil bruke informasjonsteknologien og "cyberspace" til etterretning og propaganda, og i større angrep vil tradisjonelle konvensjonelle våpen dominere, men cyberangrep kan brukes som en *del* av angrepet.

Forskere som kommer med trusselvurderinger om sannsynlighet for cyberangrep av cyberterrorister mener som oftest at trusselen øker ettersom ulike samfunnsfunksjoner blir mer avhengige av datasystemer forbundet i nettverk. Terroristgrupper og organisasjoner kan velge å bruke cyberteknikker ved å gå til angrep på datasystemer for å utvinne penger, oppnå tilgang på sensitive opplysninger under innsamling av etterretningsdata, eller å ødelegge data for å skape forferdelse og få publisitet (Hirst 1998).

Terrorister har tradisjonelt hatt politiske og/eller religiøse motiver, men også økonomiske. Politisk påvirkning og politisk endring blir nevnt som to mulige hensikter i Flynts (2000) artikkel og gjengitt i figur 2. Mange terrorister har fortsatt slike hensikter, men ved bruk av Internett og informasjonsvåpen som middel er det sannsynlig at de vil benyttes til etterretning og propaganda. De kan også få finansiell gevinst fra propagandavirksomheten som kan støtte deres videre planer og aksjoner. Hackere og stater kan ha andre hensikter enn terrorister. De fleste hackere hacker ikke med politiske hensikter, men for å vise hva de kan og øke sin prestisje. Hackere med

[28] RAND står for en sammentrekning av "research and development" og er en ikke-kommersiell institusjon som skal bidra til policy og beslutningstaking gjennom forskning og analyse.

”onde” baktanker finnes selvfølgelig og man antar at disse kan forventes å hacke seg inn på infrastruktur (f.eks. bank og finans), eksempelvis for å få økonomiske fordeler.

5.2 Analyse av empiriske eksempler

Dette delkapittelet med empiriske eksempler er som det ble nevnt innledningsvis i kapittelet er ment for å bygge opp om et potensielt trusselbilde. Tanken er å undersøke om trusselvurderingene som er ytret og beskrevet ovenfor har rot i virkeligheten. Problemet er at flere forskere har uttalt at verden ikke hittil har sett eksempler på cyberterroristangrep (i henhold til definisjonen, som blant annet innehar aspektet *frykt*; sentralt i terrorismebegrepet). Dette er kommentert innledningsvis i kapittelet. Framstillingen nedenfor vil derfor inneholde eksempler på såkalte cyberangrep. Enkelte vil hevde at noen av disse eksemplene *er* cyberterrorisme, andre hevder at de ikke er det. Jeg definerer imidlertid eksemplene ut i fra Dennings definisjon av cyberterrorisme (se 4.1.3), og vil derfor måtte si meg enig i blant annet Denning og Lia som hevder at dette ikke cyberterroristangrep. Flere av eksemplene jeg viser har større grad av hacking enn terrorisme i seg. Selv om det er terrorister som står bak cyberangrep og bruker såkalte cybervåpen, er det ikke nødvendigvis cyberterrorisme ettersom enten målet ikke er en sentral verdi som er truet, eller hensikten ikke er å skape frykt. Det har likevel vært nødvendig å søke etter lignende eksempler som har *elementer* av cyberterroristangrep i seg, eller angrep som av noen faktisk *ytres* som et cyberterroristangrep. Dette for å se nærmere på talehandlinger knyttet til konkrete, empiriske hendelser relatert til cyberterrorisme, ikke bare teoretiske ytringer om et fenomen. I mange tilfeller framstiller media det jeg, og flere forskere med meg, definerer som hacking som cyberterrorisme. Så selv om eksemplene ikke viser til cyberterroristangrep, er de verdifulle for forståelsen av det potensielle trusselbildet som blir skapt.

Eksemplene blir presentert etter hvilken aktør (terrorister, hackere og stater) som utgjør trusselen. Innenfor hvert avsnitt ser vi på hvilke midler, mål og hensikter som kan knyttes til aktørenes handlinger der det er mulig å si noe om disse. Det er primært

blitt søkt etter angrep utført av de overnevnte trusselaktørene med *cybervåpen* som middel, og det er derfor ikke med eksempler på angrep med bomber som middel, noe vi vet det finnes mange av (og som vi bl.a. har sett på Bali i Indonesia, i Israel, i Spania).

5.2.1 Terrorister som trusselaktører

Nedenfor følger noen eksempler som er funnet på angrep utført av terrorister hvor cyberangrep har vært middelet. Formen for cyberangrep har vært hacking, og målene har vært ulike, men det har vært mulig å finne eksempler på infrastruktur som mål. Ulike regjeringers web-sider har vært mål for en del aksjoner, men dette regnes trolig ikke som angrep på infrastruktur.

5.2.1.1 De Tamilske Tigrene

Enkelte amerikanske etterretningsorganer hevder at det første kjente cyberangrepet utført av terrorister fant sted når den etniske Tamilgeriljaen ”oversvømte” Sri Lankiske ambassader med tusenvis av elektroniske e-post beskjeder, ca. 800 om dagen i to uker (Denning 1999:69). Tigrene gjorde dette for å ødelegge ambassadenes kommunikasjonssystemer og for å skape frykt, og de oppnådde begge deler samt å få medienes oppmerksomhet. De hacket seg også inn på web-sidene til regjeringen og endret den for å sende ut sin politiske propaganda (Potomac Proceedings Report 1998:7). Dette angrepet blir av flere kalt ”the first recorded cyber terrorist denial of service attack” (Furnell & Warren 1999:31; Potomac Proceedings Report 1998:7). Hoffman hevder at vi kun har sett *ett* eksempel på cyberterroristangrep, og det er nettopp Tamiltigrenes cyberangrep på den Sri lankiske ambassaden. Flere forskere har imidlertid hevdet at det ikke finnes noen rapporterte cyberterroristangrep i henhold til en meningsfull definisjon på cyberterrorisme (Lia & Andrésen 2000:37), jf. Dennings syn. Trusselen for cyberterrorisme er basert på oppfatninger av sårbarhet snarere enn tidligere erfaringer (ibid.). Jeg vil også stille meg kritisk til om Tamil Tigrenes angrep faktisk kan kalles cyberterrorisme. Eksemplet viser terrorister som står bak et cyberangrep, men det kan vel lite trolig regnes som en *terrorist*handling.

De Tamilske Tigrene hacket seg inn på Sheffield University i England i 1997 og brukte universitetets datasystem til å sende propaganda og samle inn penger. Andre terrorister har også brukt data som verktøy til samme formål. Tigrene gjorde dette ved å få tak i ID og passord til flere av de ansatte på universitetet og sendte e-post fra deres legitime e-post kontoer for å spørre etter penger til veldedighet i Sri Lanka (Potomac Proceedings Report 1996:4). Her er det også uklart hvordan man definerer målet for handlingen; e-post kontoer kan strengt tatt ikke defineres som infrastruktur. Hensikten var til dels politisk ved at aksjonen ble gjennomført for å spre propaganda, men først og fremst var hensikten finansiell gevinst.

5.2.1.2 De Røde Brigadene

Terrorister kan tenkes å hacke seg inn på datasystemer og ødelegge kritiske infrastrukturer eller de kan gå til fysiske angrep mot data- og telekommunikasjonssystemer. På 1970-tallet gjennomførte de italienske Røde Brigadene 27 angrep mot datasystemer i elektronikk-, data-, og våpenindustriene (Denning 1999:69). Dette har blitt kalt et cyberangrep fordi de hadde datasystemer i industri som mål, men de brukte fysiske midler framfor hacking, virus og lignende som stort sett er knyttet til cyberangrep. Når det gjelder hensikter var de politiske. Jeg mener at dette ikke er et cyberterroristangrep bl.a. fordi middelet også må ha større preg av informasjonsteknologi.

5.2.1.3 PIRA

Det finnes eksempler på tradisjonelle terroristgrupper som har angrepet infrastruktur. I 1997 hadde PIRA[29] en plan om å detonere 37 bomber over 16 elkraftverk utenfor London med det formål å kutte tilgangen på strøm til hele byen og de nærliggende områdene (Potomac Proceedings Report 1998:7). De britiske myndighetene greide å gjennomskue terroristene før de fikk utført ugjerningen og dømte dem til strenge fengselsstraffer (ibid.). Dette er ikke et eksempel på et cyberangrep i den forstand

[29] PIRA: Provisional Irish Republican Army.

siden middelet er bomber, men et eksempel på et fysisk angrep på infrastruktur. Det kan likevel brukes som en indikasjon på at terrorister i større grad interesserer seg for slike mål.

5.2.1.4 Zapatista-bevegelsen

Det finnes også såkalte ”positive” cyberangrep som Zapatista-opprøret i Mexico. Den 31.12.94 okkuperte opprørere i Zapatista-bevegelsen seks byer i Chiapas-regionen og deklarerte krig mot den mexicanske regjeringen, satte fram radikale krav, og startet en global mediakampanje for støtte og sympati ved hjelp av Internett (Ronfeldt & Martínez 1997). Regjeringen mobiliserte hæren og andre sikkerhetsstyrker og gikk inn i Chiapas. Disse hendelsene fikk representanter for menneskerettighetsorganisasjoner og andre typer ikke-statlige aktivistgrupper (NGOer) til å strømme fra USA, Canada m.fl. og til Mexico City og Chiapas – elektronisk så vel som fysisk. Eksempelet viser at den globale informasjonsrevolusjonen påvirker sosiale konflikter. NGOene samlet seg i store nettverk av transnasjonale koalisjoner for å føre en ”nettkrig” mot den mexicanske regjeringen og til støtte for Zapatista. Denne terrorist-/geriljagruppen brukte cyberangrep som middel i aksjonen, men brukte ikke rene informasjonsvåpen som definert ovenfor, men heller Internett som middel for å skaffe støtte, da som propaganda. Målet for aksjonen var den mexicanske regjering og kan ikke regnes som en infrastruktur, men hensiktene var selvsagt å oppnå politisk endring.

5.2.2 Hackere som trusselaktører

Nedenfor følger en rekke eksempler som kan *relateres* til cyberterrorisme, men her er hackere trusselaktørene som bruker cyberangrep mot både infrastruktur og andre mål. Hackernes hensikter er som regel ikke politiske slik som hos terrorister. Av og til er det vanskelig å vite hvilke hensikter hackerne har hatt, og i andre tilfeller forstår man at motivene var å skremme, få økt prestisje o l. I Storbritannia har et økende antall radiosamband-hackere skapt problemer for flytrafikken i landet (Stalsberg 2000). Hackerne opererer som falske flygeledere og melder om feil flykurs. Falske

radiosignaler som fører til feilnavigering kan få katastrofale følger og britiske luftfartsmyndigheter har anmeldt virksomheten. Radioamatørene, som kalles radiosamband-hackere i media, har greid å unngå at kontrolltårnet fanger opp de falske radiosignalene og har hacket seg inn i flyenes cockpit.

5.2.2.1 Hacking mot nasjonale datasystemer

Devost (1995) skriver at til tross for eksempler på at amerikansk nasjonal sikkerhet har blitt truet på 1990-tallet har ikke én sidestilt hendelse utgjort en vedvarende trussel. Til sammen utgjør de likevel en trussel og er bevis på at det finnes svakheter i informasjonsteknologisystemene i USA. Det er rapportert om at en 16 år gammel britisk hacker greide å infiltrere det amerikanske forsvarsdepartementets datasystem i 7 måneder uten å bli oppdaget (Devost 1995:25). Han fikk tilgang på flydesign, forskning på ballistiske våpen, personellpapirer osv. I følge Devost skrev *The Ottawa Citizen* at man antok at hackeren også hadde tilgang på sensitive og klassifiserte databaser som omhandlet detaljer angående atomkraftinspeksjon i Nord-Korea. Hvis nord-koreanerne hadde hatt tilgang på denne informasjonen kunne det fått store konsekvenser. Under Golfkrigen i 1991 greide datahackere fra Nederland å hacke seg inn på det amerikanske forsvarsdepartementets datasystemer. Det viste seg at de hadde utnyttet kjente sikkerhetshull for å få tilgang til de fleste av systemene, og den amerikanske regjeringen kjente til disse hullene, men hadde unnlatt å gjøre noe med det (Devost 1995:28). Hackerne samlet og kopierte viktig informasjon, men heldigvis for amerikanerne ble hackingen utført av læremessige årsaker, ikke av ondskapsfullhet. I en del hackermiljø er det prestisje å hacke seg inn på amerikanske institusjoner og organisasjoner som gjerne utgir seg for å være svært sikre. Men ved å legge inn et lite virus kan store skader oppstå. I 1994 greide en 16 år gammel engelsk gutt å stenge 100 amerikanske forsvarssystemer, og under Golfkrigen dirigerte en israelsk hacker (The Analyzer) to gutter fra California til å forstyrre den amerikanske troppeutplasseringen ved å angripe Pentagons systemer og en forskningslab for atomvåpen (CSIS 1998:xv). Eksemplene viser hacking mot en viktig samfunnsfunksjon i og med at hackere har brukt cyberangrep mot datasystemer i det

amerikanske forsvarsdepartementet. Den britiske hackerens hensikter er uklare, men i de andre eksemplene kom det fram at hackerne gjennomførte angrep for å lære og på grunn av prestisje; motiver som er velkjente i "hackerverdenen".

CIA, FBI og Pentagon har alle blitt angrepet av hackere og cyberterrorister, og i USA har man i flere år satt inn store ressurser for å få slutt på sabotasjevirksomheten som man frykter vil skade USAs sikkerhet. Man kan ikke godta at inntrengere fra tid til annen hacker seg inn på nasjonale datasystemer og stjeler informasjon eller saboterer. De fleste land er svært avhengig av et elektronisk kommunikasjonssystem som binder ulike deler av infrastrukturen sammen, men systemene er sårbare og må forsvares for å hindre nye typer teknologiske angrep som har kommet med Informasjonsrevolusjonen. I USA har det siden slutten av 1990-tallet blitt utgitt en rekke offentlige dokumenter angående sikring av informasjonsinfrastruktur. I 2000 etablerte det Hvite Hus en informasjonssikkerhetspolicy og i 2001 kom loven "Cyber Security Information Act" for å nevne noe (Alexander & Swetnam 2001).

5.2.2.2 Hacking mot statlige web-sider

Flere hackere har brukt virus og hacking i cyberangrep mot regjeringers web-sider. Regjeringen og dens underliggende strukturer (departementene) er viktige samfunnsfunksjoner, men det er et definisjonsspørsmål om de skal inngå i generell oppfatning av infrastruktur. Det samme vil da gjelde regjeringers web-sider som sannsynligvis ikke vil regnes som infrastruktur. Imidlertid oppfattes cyberangrep mot alle deler av regjeringen som truende. Hackere kan ønske å hacke seg inn på et datasystem for å omskrive eller stjele informasjon. Det skotske parlamentets web-side har blitt endret, og det britiske Railtracks web-side ble endret på nyttårsaften 1999 til å informere kunder om at alle tog var kansellerte (Easton 2000). Slike hendelser er irriterende og forstyrrende, men det blir først alvorlig hvis hackerne greier å infiltrere selve datasystemene og f.eks. ødelegge trafikksignaler o.l.. "In the 60's it was the bomb. In the 80's it was Aids. In the new millenium it's cyber terror" (ibid.). En portugisisk hackergruppe, PHAIT (Portuguese Hackers Against Indonesian Tyranny), hacket seg inn på den indonesiske regjeringens webside for å få oppmerksomhet rettet

mot situasjonen på Øst-Timor. På hjemmesida til regjeringen skrev de blant annet: "Welcome to the Department of Foreign Affairs, Fascist Republic of Indonesia" (Furnell & Warren 1999:32; Rathmell m.fl. 1997: avsnitt 3.1). Denne gruppa har ført mange hackerangrep mot Indonesias regjering. Under Kosovo-kampanjen samlet ulike serbiske hacker-grupper seg om å drive med massive angrep på NATO og andre vestlige regjeringers web-sider, i noen tilfeller var det så mange som 2000 e-post angrep om dagen, og av dem inneholdt flere macro-virus. Serbiske hackere forsøkte også å plante virus i Det britiske forsvarsdepartementets signal- og kommunikasjonssystemer (O'Brien 2000:10).

Det er vanskelig å spore hvem som står bak mange av hackerangrepene det rapporteres om. I følge rykter fra etterretningsorganisasjoner skal en pakistansk "Hackersz Club" stå bak angrep på statlige indiske og amerikanske web-sider ved å erstatte bilder med slagord som "Free Kashmir" (James & Cooper 2000:54). I 1996 greide en svensk hacker å lage store skader på 911-nettverket i Florida (ibid.). Den 13.03.02 hacket en gruppe hackere seg inn på daværende Direktoratet for sivilt beredskaps hjemmeside *beredskapsnett.no* her i Norge og forandret forsida til et bilde av en hjerne hvor det stod: "Attacked soul ownz you – dominating your mind" og "Olà Beredskapsnett Sorry!".

5.2.3 Stater som trusselaktører

Både nasjoner og terroristgrupper begynner i større grad å bruke cyberspace som slagmark for sine kamper og aksjoner. I Kashmir har det f.eks. vært en pågående cyberkrig ettersom India og Pakistan har ført krig i cyberspace (BBC News 1999). Folk fra begge disse landene har ført propagandakampanjer ved hjelp av Internett gjennom å sende støtende e-post og sette opp provoserende websider.

5.2.3.1 NATO under Kosovo-kampanjen

NATO er en organisasjon og i så måte ikke en statlig aktør, men siden NATO er en allianse bestående av de sentrale europeiske stater og USA blir NATO-eksemplene

tatt med under dette punktet. De NATO-allierte statene fører i stor grad en forsvarspolitikk bygd på NATOs dokumenter og bestemmelser. Under Kosovo-kampanjen hadde NATO suksess med flere taktiske og operasjonelle angrep, men informasjonsoperasjoner (IO) ble ikke utnyttet godt nok, og i følge admiral Ellis: ”properly executed, IO could have halved the length of the campaign but the IO operators were too junior and from the wrong communities to have the required impact on planning and execution” (sitert i O’Brien 2000:5). NATO kunne ha brukt mange midler som f.eks. mikrobølgeteknologi for å ødelegge Beograds elektroniske utstyr samt logiske bomber, trojanske hester, virus m.m. for å ødelegge eller stenge jugoslaviske militær- og regjeringsnett (O’Brien 2000:6). Det som faktisk skjedde var at Pentagon holdt seg til ”Powell-doktrinen” som innebærer at USA bare skal intervenere når de kan mønstre overveldende makt. IO ble brukt i begrenset grad, og først og fremst innen propaganda. Likevel mislyktes NATOs propaganda-kampanje, hovedsakelig fordi Beograd hadde total kontroll over innenlands media og kringkasting. Innen offensiv informasjonskrigføring lyktes de i noe større grad: ”Soft kill” våpen, slik som grafittbomber[30], ble brukt mot kraftforsyningen, de sendte ut fly som slapp bomber over kraftverk den 2. mai 1999, de hacket seg inn på den serbiske regjeringens e-post system, og de infiltrerte internettsystemer i banker (Grunnan 2000:15).

Den elektroniske krigføringen ble vurdert som vellykket. Det serbiske telefonnettverket brøt sammen slik at det militære ble tvunget til å kommunisere med mobiltelefoner, og de trengte seg inn i det jugoslaviske luftforsvarsnettet ved hjelp av jamming og la inn virus i mikrobølgenettet. Slik fikk jugoslavene problemer med å komme seg inn på sine egne datanettverk og dermed minsket deres muligheter til å treffe nøyaktig på mål i lufta (O’ Brien 2000:8). I tillegg hacket amerikanske hackere fra CIA og NSA seg inn på e-post systemet til den serbiske regjeringen for å få et

---

[30] Definisjon fra Wikipedia, The Free Encyclopedia (http://en.wikipedia.org): A **graphite bomb** (also known as the "Blackout Bomb" or the "Soft Bomb") is a non-lethal weapon used to disable electrical power systems. Graphite bombs work by spreading a cloud of extremely fine, chemically-treated carbon filaments over electrical components, causing a short-circuit and a disruption of the electrical supply.

inntrykk av hva man tenkte i Beograd, og de infiltrerte internettsystemet til banker over hele verden for å finne kontoer som tilhørte serbisk lederskap. De ønsket å kartlegge Milosevics aktiva og finansielle kapabiliteter, og disse aktivitetene ble videreført av etterretningstjenesten etter konflikten. Ingen finansielle aktiva ble tatt under konflikten fordi man fryktet at det ville skape ytterligere destabilisering i Jugoslavia.

Hovedårsaken til at USA og NATO ikke brukte IO i større utstrekning i Kosovo skyldes legalitetshensyn. Ved å bruke datavirus og EMP-våpen[31], samt å sikte seg inn på elektroniske distribusjonsnetteverk, kunne man risikere å treffe eller påvirke sivile, og dette ville ha vært et brudd mot Génève-konvensjonen[32] (O'Brien 2000:9). Siden angrep med bruk av overnevnte teknikker kunne bli oppfattet som å sikte på sivile, ble de i stor grad unngått. Hvordan man skal lage retningslinjer, lover og regler for bruk av IO vil bli en debattert sak i lang tid. Innen NATO har det blitt utgitt en rekke IO policy-dokumenter og doktriner i årene 1998-2005, og de viser at en felles forståelse av informasjonsoperasjonsbegrepet er i ferd med å etableres i NATO-organisasjonen og blant nasjonene (NATO, RTO 2006: ES-1). Forskere diskuterer også seg i mellom om hvordan man best kan skape samarbeid og om mulig et felles lovverk. I litteratur som beskriver midler som ble brukt under Kosovo-kampanjen henviser de fleste til informasjonsoperasjoner framfor cyberangrep. Inntrykket er at cyberangrep brukes om angrep utført av ikke-statlige aktører, mens informasjonskrigføring og informasjonsoperasjoner brukes om angrep utført av statlige aktører. NATO bruker informasjonsoperasjoner framfor informasjonskrigføring, og derfor har det ordet blitt brukt i eksemplene det refereres til. Selv om ordet på selve angrepet er forskjellig inngår de fleste samme midlene i et cyberangrep og i en informasjonsoperasjon. Hacking og virus kan like gjerne benyttes som middel i en informasjonsoperasjon. NATO brukte informasjonsoperasjoner i

[31] EMP: Elektromagnetisk puls våpen.

[32] Génève-konvensjonen innebærer (blant annet) at man ikke skal sikte seg inn på sivile/ha sivile som mål under konflikter.

form av propaganda, grafittbomber, hacking, jamming og virus (en blanding av fysiske og ikke-fysiske virkemidler) mot infrastruktur som kraftforsyning og banker samt den serbiske regjeringens e-postsystem. Hensiktene var politiske og økonomiske. NATOs handlinger under Kosovo-krisen skapte et behov for en inngående diskusjon om bruk av informasjonsoperasjoner. NATO brukte ulike typer informasjonsoperasjonsvåpen, f.eks. grafittbomber mot infrastrukturen for å frata sivilbefolkningen elektrisitet og dermed skape press på den jugoslaviske regjeringen. Dette førte til at befolkningen ble fratatt en av sine viktigste livsstøttende fasiliteter.

5.2.3.2 Serbia under Kosovo-kampanjen

De viktigste serbiske informasjonsoperasjonene bestod av ”perception management” og propaganda, samt hacking og ”denial of service”-angrep på vestlige og Nato web-sider og introduksjon av virus på NATOs e-post system. Dette ble kalt ”info-war” i mediene, men det var aldri en koordinert informasjonskampanje (Grunnan 2000:15). Den jugoslaviske regjeringen brukte store krefter på å styre borgernes oppfatninger av krigen, og noen spede forsøk ble gjort på å påvirke oppfatninger rundt om i verden ved å sponse pro-serbiske websider og ”chat-rooms”. Jugoslavene lot til å lykkes med å styre oppfatningene til sin egen befolkning, og ved å sponse pro-serbiske web-sider og ”chat-rooms” greide de å påvirke oppfatninger utenfor Jugoslavia. Det serbiske informasjonsdepartementet hadde web-sider med informasjon om ”albansk terroristaktivitet”, og serberne viste også videoer av kosovoalbanernes leder, Ibrahim Rugova, i møte med Milosevic, dette for å forvirre Vesten og KLA[33] om Rugovas intensjoner (O’Brien 2000:10).

5.3 Oppsummering

Globaliseringen har skapt muligheter for flyt av varer, tjenester, informasjon og teknologi over landegrensene, og framveksten av Internett har gjort det lettere å

[33] KLA: Kosovo Liberation Army.

kommunisere. Dette har skapt nye muligheter og gitt ulike grupperinger, som f.eks. terroristorganisasjoner, større spillerom til å øke sin slagkraft (Lia 2000:12). Et nytt trusselbilde har blitt dannet som følge av informasjonssamfunnets oppblomstring, som igjen har skapt sårbare samfunn og nye midler for å utnytte denne sårbarheten på.

Hoffman påpekte at antallet drepte pga. terrorisme har gått ned på 1990-tallet i forhold til 1980-tallet, mens trusselsoppfatningene er mye større en noen gang (Lia & Andrésen 2000:26). Det kan se ut som om kritisk infrastruktur ikke er et stort mål for politiske terrorister, men man kan selvfølgelig ikke utelate muligheten for at de vil angripe denne type mål. Terrorister kan ha politiske hensikter dersom de bruker de nye informasjons-/cybervåpnene, men det kan være de vil bruke disse midlene som et ledd av et større angrep, kanskje sammen med tradisjonelle konvensjonelle våpen.

For dagens terrorister finnes muligheten å lage web-sider fordi det er billigere å publisere propaganda via nettet framfor å sende informasjon til tilhengere som befinner seg langt unna geografisk, de kan drive pengeinnsamling til saken sin, og man kan lage web-sider fra hvor som helst, f.eks. i et land som støtter terrorisme (Hirst 1998). Internett er i stor grad tilgjengelig for alle og det blir ansett som sannsynlig at enkelte terroristgrupper vil bruke nettet til å legitimere seg selv samt å drive sin virksomhet med utgangspunkt i nettsidene sine. Via nettet er det også svært lett å oppdrive informasjon om ulike hackingmetoder som spoofing, sniffing, trojanske hester osv. Dennis (1998) skriver i en artikkel om ”Globalization Process and Acquisitions of New Technology” at så snart terroristgrupper har skaffet til veie informasjon om cybervåpen via nettet er det slettes ikke en selvfølge at de bare blir brukt på Internett. Han konkluderer med at ”the Internet may bring a new era for terrorism and it should be taken very seriously”.

I dette kapittelet er det gjort forsøk på å vise at den nye cybertrusselen har blitt generert som følge av utviklingen av ny teknologi og vår avhengighet av denne. Den nye teknologien skaper grobunn for oppblomstring både av nye trusselaktører (hackere) og nye midler, og midlene er tilgjengelige for tradisjonelle så vel som nye trusselaktører. Det *er* en mulighet for at cyberterroristangrep i henhold til Dennings

definisjon kan skje. Selv om vi ikke har sett eksempler på rene cyberterroristangrep så langt, kun lavskala-cyberangrep, viser eksemplene i dette kapittelet at det utvilsomt er et potensielt trusselbilde knyttet til cyberterrorisme. Men utgjør talehandlingene om den mulige trusselen en reell sikkerhetstrussel? Det skal vi se nærmere på i neste kapittel hvor det blant annet drøftes om fullstendig sikkerhetisering av cyberterrorisme har funnet sted på bakgrunn av diskursen rundt begrepet.

6. Diskursen rundt begrepet cyberterrorisme i ulike kontekster

Hovedpoenget med dette kapittelet er å undersøke og analysere de kontekster og fora hvor begrepet cyberterrorisme finnes og brukes. Hensikten er å framstille offentlige ytringer/uttalelser relatert til problemet cyberterrorisme som kan tolkes som talehandlinger (”speech acts”) som kan ha som hensikt å ”sikkerhetisere” cyberterrorisme. Talehandlinger som innbefatter ord som cyberterrorisme, cyberangrep, informasjonskrigføring m.m., og som presenterer disse som en utfordring, trussel eller risiko vil derfor stå sentralt. Dette materialet skal brukes til å analysere *hvem* som ”snakker” trusler, *hvordan* og i hvilken *kontekst* de gjør det.

Kapittelet innledes med en kort introduksjon av de sikkerhetiserende aktører og kontekster hvor diskursen som her studeres foregår (6.1). Cybertruslene sies ofte å komme fra terroristgrupper, hackere, kriminelle osv. fordi det er disse som kan true ved hjelp av de nye midlene som finnes. De sikkerhetiserende aktørene ytrer seg om disse gruppene og alvoret av truslene. Ytringene, altså talehandlingene, til de sikkerhetiserende aktørene blir sentrale i denne forbindelsen. Ordene de bruker og måten de tolkes på er avgjørende for hvordan cyberterrorisme blir oppfattet som en sikkerhetstrussel. Jeg har valgt å gjengi diskurser om cyberterrorisme sett fra to ulike kontekster, akademisk nivå (6.2) og politisk nivå (6.3), og talehandlingene er organisert i forhold til en rekke momenter. Media kunne vært brukt som en tredje kontekst, men jeg kommer tilbake til problematikken rundt bruken av media som sikkerhetiseringsnivå nedenfor. Deretter diskuteres om cyberterrorisme kan sies å ha blitt sikkerhetisert og etablert som en del av den sikkerhetspolitiske agenda (6.4), og avslutningsvis vil det bli gitt en oppsummering av diskursanalysen (6.5).

6.1 Sikkerhetiserende aktører og kontekster hvor diskursen foregår

I en sikkerhetiseringsprosess må de sikkerhetiserende aktørene defineres fordi det er de som sikkerhetiserer saker og definerer referanseobjekter som truet (se kap.2). I henhold til teorien har stater tradisjonelt blitt sett på som referanseobjekt og aktørene har generelt vært regjeringer, politikere og pressgrupper osv. Jeg velger å se på politikere, forskere og delvis mediefolks rolle som sikkerhetiserende aktører. Disse aktørene har relevans til de tradisjonelle sikkerhetiserende aktørene, og det virker som om det meste av diskursen rundt begrepet cyberterrorisme foregår innenfor *kontekstene* de tilhører. Forskerne opererer i en akademisk kontekst, politikerne og andre politiske og offentlige beslutningstakere opererer i en politisk kontekst, og journalister opererer i en mediekontekst. Det må likevel understrekes at disse aktørene ikke er uavhengige. Politikeren refererer og tolker forskerens resultat og journalisten skriver om dette i media. Jeg benytter meg av to hovedkontekster eller *nivåer*; akademisk og politisk/administrativt. Tanken var å operere med et eget medienivå i tillegg, men jeg har valgt å inkludere det i de to andre nivåene (som et moment jeg har kalt mediediskurs) ettersom media kan ha en dobbeltrolle. Jeg bruker med andre mediekildene (se 3.4.3), selv om det ikke vises i et eksplisitt analysenivå. Journalister gjengir i stor grad intervjuer med, eller dokumenter skrevet av, forskere, personer i det politiske liv og statsadministrasjonen, og dette kan tolkes som ”speech acts” og gir dem en rolle som sikkerhetiserende aktører. De kan selvsagt også ytre egne meninger og publisere egne analyser basert på informasjon fra forskere og politikere, og da opptrer journalistene utvilsomt som selvstendige sikkerhetiserende aktører. Samtidig må det påpekes at media lever av å skape et trusselbilde. Denne dobbeltrollen gjør at det blir vanskelig å analysere diskursen om cyberterrorisme i en mediekontekst, og jeg har derfor utelatt dette nivået. Det må dessuten bemerkes at det bare er politikere som kan iverksette tiltak som går utover det legitime, og således bare de som kan fullstendig sikkerhetisere. Forskere og mediefolk kan bare ha ”speech acts” og være med på sikkerhetiseringsprosessen. Politikere kan derimot ha begge deler, både komme med ”speech acts” og komme med tiltak, og dermed være de som

sikkerhetiserer en sak. Det er opp til politikere og embetsverket å akseptere talehandlinger fra andre sikkerhetiserende aktører og gjennomføre tiltak. Pressedekning bestemmer likevel noe av *gjennomslagskraften* politikere og forskere har som sikkerhetiserende aktører, og media kan også fungere som en pressgruppe for å få iverksatt tiltak. Se 6.5 for utførlig drøfting av sikkerhetiseringproblematikken rundt begrepet cyberterrorisme.

Innenfor hver av kontekstene akademisk og politisk nivå vil jeg drøfte diskursen som går på syn i forhold til trusler, midler, mål og hensikter (punkter fra kap.5) i relasjon til cyberterrorisme. Disse forholdene blir organisert inn i en rekke momenter: hva, hvorfor og vurdering av trusselen, konsekvenser, framtidsperspektiv, mediediskurs og begrepsbruk/nøkkelord.

6.2 Diskurs på akademisk nivå

Diskursen blant akademikere angående trusselen for cyberterrorisme og informasjonskrigføring er levende, og blant denne gruppen sikkerhetiserende aktører gjenspeiles ulike syn. De fleste anser trusselen som reell, men det er ulike oppfatninger av hvor store konsekvenser et cyberterroristangrep vil kunne få, når vi vil få se et slikt angrep, og hvor vanlige slike angrep vil bli. Nedenfor følger hovedpunkter fra diskursen med utsagn fra akademikere som står sentralt i debatten. Analysen skal forsøke å gi svar på hvordan ”speech-actene” (talehandlingene) til denne gruppen sikkerhetiserende aktører er med på å sikkerhetisere cyberterrorisme og få det til å framstå som en eksistensiell trussel. I analysen søker jeg derfor å studere ulike momenter ved ytringene til aktørene.

6.2.1 Hva er trusselen?

Under dette punktet vil fokus ligge på fra hvem/hvilke aktører trusselen kommer fra, og de fleste akademikere nevner ikke-statlige aktører som hackere, kriminelle og terrorister som de som skaper trusselen. Khalilzad (1999) hevder at individer (her ser man for seg hackere) med ulike hensikter (utfordringer, moro, penger, hevn),

terrorister, kriminelle, ad hoc-grupper og stater blir ansett som de mest reelle trusselaktørene. Disse gruppene kan tenkes å utvikle og bruke informasjonskrigføringsteknikker. Koordinerte grupper og stater vil sannsynligvis ikke benytte seg av enslige hackere, men heller gjennomføre koordinerte angrep med mange repetisjoner ved hjelp av ulike agenter. ”The possibility of damage from multiple, coordinated attacks exceeds the potential damage from individual attackers focused on single targets” (Khalilzad 1999:409). Videre hevder Khalilzad at ”coordinated groups and states could disrupt U.S. military operations and threaten parts of the U.S. civilian infrastructure” (ibid.). Libicki (1995) er også opptatt av at hackere er sentrale aktører i forbindelse med cyberangrep. Disse kan for så vidt gjennomføre både hacker- og cyberkrigføring, men i cyberkrigføring kan andre aktører, som f.eks. terrorister, også stå bak.

I artikkelen ”Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” prøver Denning å vise hvordan Internett blir brukt av de aktørene som ønsker å påvirke eller endre utenrikspolitikk. Hun legger vekt på de ikke-statlige aktørene og deler deres aktiviteter i tre kategorier: aktivisme, hacktivisme og cyberterrorisme. Aktivisme referer til normal, ikke-ødeleggende bruk av Internett for å støtte eller fremme en sak, hacktivisme referer til en blanding av hacking og aktivisme, og cyberterrorisme refererer til ”konvergensen av cyberspace og terrorisme” (Denning 2000). Grensene mellom disse kategoriene er vage, ”for example, an e-mail bomb may be considered hacktivism by some and cyberterrorism by others” (ibid.). Hun sier videre at en aktør kan handle på tvers av kategoriene, som f.eks. at en terrorist kan bruke virus som ledd i en større cyberterroristkampanje. Bruk av virus og datanettverksangrep (”computer network attacks”) som er ansett som verktøy i hacktivismekategorien er også relevant for terrorister.

Center for Strategic and International Studies, CSIS (1998), henviser til en trusselvurdering foretatt av Defense Science Board, som delte de ulike truslene USA stod overfor fra hackere, terrorister osv., inn i fire ulike kategorier: 1) at det var

bekreftet at trusselen eksisterte, 2) at det var sannsynlig at trusselen eksisterte, men at det ikke var bekreftet, 3) at trusselen var sannsynlig før år 2005, og 4) at trusselen var usannsynlig før år 2005. Når det gjelder terroristgrupper ble denne trusselen ansett som sannsynlig under kategorien ”sannsynlig at trusselen eksisterer, men det er ikke bekreftet”. Videre hevder CSIS at terroristgrupper med en hang for teknologi vil med større sannsynlighet enn andre være tilbøyelige til å bruke informasjonskrigføring, og dermed øker muligheten for angrep mot informasjonsbaserte mål betraktelig. Mange terroristgrupper har web-sider og har forstått hvor mye makt som ligger i det globale informasjonsnettverket. Flere grupper som Zapatistene og Tamil Tigrene har benyttet seg av datakunnskap i sine kampanjer. ”Terrorists, insurgents, and radicals have long understood the importance of infrastructure to societies and have placed it high on their target lists. The United States should expect that information systems will be no exception”(CSIS 1998:26).

6.2.2 Hvorfor finnes trusselen?

Det er ulike oppfatninger av hvorfor trusselen for cyberangrep og informasjonskrigføring finnes. Selv om mange forskere hevder at det eksisterer en trussel fra f.eks. terrorister, er de ikke alltid like opptatt av å forklare hvorfor denne trusselen har oppstått. Khalilzad (1999) påpeker at den globale konteksten har blitt svært kompleks etter Den kalde krigen, og det har skapt grobunn for framvekst av flere ulike aktører. CSIS har hatt et prosjekt på global organisert kriminalitet og har i den forbindelse også utgitt et forskningshefte om cyberkriminalitet, cyberterrorisme og cyberkrig. I denne utgivelsen blir det hevdet at USA står ovenfor nye trusler som de aldri før har sett og trusselen er strategisk informasjonskrigføring[34]. Den nye trusselen blir betraktet som et direkte resultat av Informasjonsrevolusjonen.

[34] Strategisk informasjonskrigføring blir av CSIS omtalt som ”muligheten for koordinerte, systematiske angrep mot USA gjennom datamaskiner, kommunikasjonssystemer, databaser og media”.

6.2.3 Vurdering av trusselen

Akademikerne, eller forskerne, vurderer truslene på ulik måte med hensyn til hvor reell og eventuelt hvor alvorlig de mener den er osv. Vurderingene er hos mange preget av usikkerhet, mens andre virker sikre i sine vurderinger. Både Vatis og Khalilzad er forskere som mener at trusselen for cyberterrorisme og informasjonskrigføring er økende og reell. Årsakene til dette er at kritiske infrastrukturer har blitt nye mål og teknologiutviklingen har skapt nye våpen. Vatis' kommentarer kom i forbindelse med et seminar om cyberterrorisme og informasjonskrigføring organisert av Potomac Institute for Policy Studies og Terrorism Studies Program ved George Washington University i 1998. På seminaret uttalte han: "I think the threat is real and I think it's growing", og fortsatte med: "It is just as easy now to engage in a cyber attack from Tehran as it is from Toledo, Ohio"(Potomac Proceedings Report 1998:4). Han hevder at man ikke trenger å være en dataekspert for å gå til en hacker-webside og laste ned "hacking-oppskrifter". Med andre ord, teknikken er tilgjengelig og blir stadig mer tilgjengelig etter som vi blir del av den globale informasjonsinfrastrukturen. Det er hovedsakelig økningen i antall tilgjengelige mål som beviser at trusselen er økende, i følge Vatis. Han sier likevel at det ikke er mange eksempler på terrorister som fører cyberangrep og bruker cybervåpen ennå. "I think the use of cyber tools by traditional terrorists are still relatively few in number"(ibid.:7). Han nevner et par-tre eksempler på terrorister som har brukt cyberangrep, blant annet Zapatista-opprøret og eksemplet med de Tamilske Tigrene på Sri Lanka, men disse eksemplene har jeg ikke tidligere karakterisert som cyberterroristangrep (se kap.5). Angrepet av de Tamilske Tigrene på den sri lankiske regjeringens Internettsider har av mange blitt kalt det første (og eneste) rapporterte cyberterroristangrep, men jeg har tidligere stilt spørsmålstegn ved om det kan kalles det. Det er spesielt i media at dette angrepet har fått stor oppmerksomhet, kanskje fordi media har behov for å vise konkrete eksempler på de truslene som forskerne hevder er reelle.

Khalilzad skriver:”The information-warfare threat is increasingly real. Extremely sophisticated information-warfare tools have become freely available over the Internet” (Khalilzad 1999:406). Han hevder at til og med nybegynner-hackere kan finne systemsvakheter som det tidligere tok mange års erfaring å finne. Libicki hevder at framtidas konflikter vil bli karakterisert av kamp om kontroll og dominans av informasjonssystemer. Boka ”What is Information Warfare?” som kom ut i 1995 begynner med følgende:

”In recent years, a concept known as ”information warfare” has become popular within certain circles of the U.S. defense establishment. The concept is rooted in the disputable fact that information and information technologies are increasingly important to national security in general and to warfare especially” (Libicki 1995:ix).

Libickis betraktninger viser at spørsmål rundt informasjon og informasjonens viktighet i krigføring var på dagsordenen også i første halvdel av 1990-tallet. Libicki er opptatt av å definere informasjonskrigføring og har skilt ut sju mulige former for informasjonskrigføring som han studerer nærmere, og disse er: kommando- og kontrollkrigføring, etterretningsbasert krigføring, elektronisk krigføring, psykologisk krigføring, hackerkrigføring og cyberkrigføring. Han sier at de som søker en idealdefinisjon må lete et annet sted – ”information warfare may better be considered a mosaic of forms, rather than one particular form” (Libicki 1995:6). Av de sju formene for informasjonskrigføring Libicki tar for seg vil de to sistnevnte være av størst interesse for diskursen jeg studerer.

Både Denning og Rathmell stiller spørsmål ved om cyberterrorisme *er* framtidas trussel. Når det gjelder svar på spørsmålet hevder Rathmell at ”the convergence of current conventional wisdoms regarding technological and socio-political developments suggests that it may be”(Rathmell 1997). Videre henviser han til Schwartau og Laqueur og sier:”If warfare is going to be conducted in cyber-space and if the combatants of the future are going to be irregulars, then cyber-terrorism is the logical paradigm of future conflict”(ibid.). Han påpeker at for å forstå utstrekningen av den framtidige trusselen fra cyberterrorisme må man ikke sluke alle uttalelsene fra futuristene, men foreta strategiske analyser. Denning er opptatt av at det finnes *få*

bevis på at terrorister har brukt cybervåpen, Internett og liknende hjelpemidler i ulike sammenhenger for å skape alvorlige konsekvenser. Selv om flere og flere terroristgrupper bruker Internett for å kommunisere, koordinere sine aktiviteter, samle inn penger og drive propaganda, sier Denning følgende: ”There is little concrete evidence of terrorists preparing to use the Internet as a venue for inflicting grave harm” (Denning 2000). Dennings utsagn skulle indikere at hun betrakter trusselen for cyberterroristangrep som tilstedeværende, men at vi ikke vil se alvorlige angrep i nær framtid. Hun sier selv at ”there have been few if any computer network attacks that meet the criteria for cyberterrorism” og mener at det nærmeste man har vært er eksemplet med det Tamilske Tigrene (Denning 2000). Videre påpeker hun at ”given that there are no instances of cyberterrorism, it is not possible to assess the impact of acts that have taken place”(ibid.). Selv om det ikke er rapportert om hendelser som kan kalles cyberterrorisme uttaler Denning at: ”What can be said is that the threat of cyberterrorism, combined with hacking threats in general, is influencing policy decisions related to cyberdefense at both a national and international level”(Denning 2000).

Ettersom samfunnet har blitt mer avhengig av informasjonsteknologi har informasjonskrigføring vokst fram som et middel i framtidige konflikter. I den forbindelse blir cyberterrorisme betraktet som ”a logical application of IW [information warfare]”(O’Brien & Nusbaum 2000:50).

”As the technological and socio-political trends converge through more complex and efficient means, it is possible that cyber-terrorism is the logical paradigm of future conflict. Fortunately, the potentially devastating consequences of cyber-terrorism have not yet occured” (O’Brien & Nusbaum 2000:55).

Det er spesielt den senere tids virus- og hackingangrep som har bevist hvor sårbart data-og nettverkssystemet selv om de som har stått bak har oppnådd forholdsvis lite med det. Likevel har mye oppmerksomhet blitt gitt tanken om at cyberterroristangrep mot kritisk infrastrukturer vil bli det viktigste paradigme ved framtidig asymmetrisk krigføring (O’Brien & Nusbaum 2000:50). ”What makes cyber-terrorism unique in the realm of terrorism is the ease with which vast amounts of damage can be inflicted

on a technological infrastructure by actors who are great distances from the target"(O'Brien & Nusbaum 2000:54).

"It is this combination of widely available capabilities and U.S. vulnerability coupled with inadequate defenses that make the potential threat of information warfare so great" (CSIS 1998:1). Denne kommentaren fra CSIS viser at de mener det eksisterer en potensiell trussel for informasjonskrigføring og liknende scenarier. CSIS drøfter også påstander som har kommet fra flere hold om at USA er sårbar overfor et "elektronisk Pearl Harbor". De kaller dette et "bolt-out-of-the-blue scenario" og anser ikke dette som den største trusselen USA er utsatt for (CSIS 1998:2). En større trussel kommer fra en nøye planlagt og eksakt utført kampanje fra en nådeløs og fokusert motstander som har en sofistikert forståelse av hva informasjonskrigføring går ut på (ibid.). "The more significant information warfare threat would likely resemble not Pearl Harbor but instead Waterloo, where technology, planning, and careful execution were used as part a long-range plan aimed at altering the world's political, military, and economic order" (ibid.). CSIS drøfter om det faktisk eksisterer en trussel for strategisk informasjonskrigføring og mener trusselen har fått økt oppmerksomhet den siste tiden (deres rapport ble gjennomført i 1998), men likevel har mange funksjonærer vært sene med å godta at det finnes en alvorlig trussel for strategisk informasjonskrigføring og mange er fortsatt i tvil (CSIS 1998:21).

6.2.4 Konsekvenser

Når det gjelder hvor stort problem cyberterrorisme er og om det kommer til å bli et stort problem i framtida, svarer Denning (2000) naturlig nok ikke eksakt på det, men hun påpeker de komparative fordelene ved cyberterrorisme framfor fysiske metoder. Et cyberterroristangrep kan utføres hvor som helst, anonymt, billig, og man må ikke behandle eksplosiver eller foreta en selvmordshandling i forbindelse med angrepet. Det vil trolig bli stor medieoppmerksomhet rundt et slikt angrep selv om bomber ikke er involvert, for media ser ut til å være opptatt av alle former for dataangrep og det

kan regnes som en fordel. En ulempe kan være at man ikke får full kontroll over angrepet og ikke oppnår ønsket ødeleggelsesnivå fordi datasystemer er komplekse. I boka *Information Warfare and Security* tar Denning opp ulike aspekter ved informasjonskrigføring. Hun er opptatt av at informasjonskrigføring ikke er et nytt begrep, at det ikke er et "third wave" fenomen eller et resultat av datarevolusjonen (Denning 1999:13). Mennesker har til alle tider vært opptatt av å beskytte viktig informasjon, men det må sies at informasjonskrigføringen har blitt omformet som følge av ny teknologi og utvikling innen media og kommunikasjon (Denning 1999:14). Den nye teknologien har først og fremst skapt flere muligheter og mål for de som ønsker å føre informasjonskrigføring, men har også ført til større avhengighet av teknologi som dermed blir sårbar hvis noe skulle skje. "The big question is: Can someone launch an attack with catastrophic consequences and, if so, what are the chances of that happening? In truth, nobody knows"(Denning 1999:19).

6.2.5 Framtidsperspektiv

De sikkerhetiserende aktørene har ulike perspektiver på framtida; når de tror vi vil få se et alvorlig cyberangrep, hvor vanlig det kommer til å bli osv. Khalilzad (1999) ser ikke for seg et "elektronisk Pearl Harbor" med det første, men påpeker at informasjonsvåpen som kommer i gale hender, f.eks. hos rivaliserende regionale makter, kan få stor strategisk betydning også for amerikansk nasjonal sikkerhet. Denning hevder at ingen virkelig vet om noen kan gjennomføre et alvorlig angrep, men det er sikkert at informasjonssystemene er sårbare og at det er folk som er motivert til å gjøre forferdelige handlinger. Derfor må man forberede seg på en usikker framtid (Denning 1999:19). Trusselen er tilstedeværende, men hun tror ikke vi vil få se angrep i nær framtid på grunn av få rapporterte angrep tidligere. O'Brien & Nusbaum (2000) uttaler ikke når de tror verden vil få se alvorlige cyberterroristangrep, men siden de uttaler at "cyberterrorisme er et logisk paradigme av framtidig konflikt" kan det tolkes dit hen at de i alle fall ser det som *sannsynlig* at cyberterrorisme vil bli aktuelt "en gang" i framtida. Når det gjelder

framtidsperspektiv referer CSIS til den mest omfattende trusselvurderingen som hadde blitt gjennomført i USA inntil rapporten ble skrevet (1998). En arbeidsgruppe fra Defense Science Board rapporterte at USA sto overfor en signifikant informasjonskrigføringstrussel fra hackere, kjeltringer og kriminelle, men konkluderte med at trusselen fra mer alvorlige former for informasjonskrigføring så ut til å være lave de neste 5-10 årene (CSIS 1998:21).

6.2.6 Mediediskurs

Mange mennesker er opptatt av hvordan terrorister kan bruke Internett for å angripe en fiendes informasjonsinfrastruktur. The Christian Science Monitor har snakket med en professor ved University of North Carolina, Alan Freitag, som mener det er like viktig å diskutere hvordan terrorister bruker Internett for å spre sitt budskap. Han sier: ”the seizure of the Japanese embassy in Lima, Peru by the Tupac Amaru group was the first use by a terrorist organization of a Web site in support of a terrorist act” (Regan 1999). Medlemmer fra gruppen tok i desember 1996 mange gisler i ambassaden og holdt 75 av dem fanget i fem måneder. Selv om ikke store deler av verden var online i 1996, innså de at media brukte Internett og slik kunne de raskt spre budskapet til pressen og dermed til publikum. Freitag påpeker at medieorientert terrorisme vokste fram på 1980-tallet, men terrorister ble ofte frustrerte fordi media ikke alltid fortalte historien slik de ønsket det, og med framveksten av World Wide Web kunne de overliste mediefolket og spre usensurert materiale til folket (ibid.). Dette eksemplet viser indirekte at media er med på å sikkerhetisere uttalelser fra forskere, selv om det likevel er forskerens sin diskurs. Media er med på å vise et eksempel hvor terrorister tar i bruk data og Internett i forbindelse med en terroristhandling.

En rekke sikkerhets- og teknologieksperter har uttalt at trusselen fra cyberterrorisme har blitt ”overhyped”(BBC News 2003), og når det gjelder private selskaper og firmaer er de først og fremst utsatt for ordinære kriminelle og kjeltringer framfor cyberterrorister. De mener at å stoppe e-poster o.l. ikke kan kalles terroraksjoner.

”The hype is coming from the US Government and I don’t know why”, uttaler en respektert sikkerhetsekspert, Bruce Schneier (ibid.) Dette er et eksempel på at media også gjengir uttalelser fra sikkerhetseksperter utenfor det rent akademiske miljø, men som heller ikke kan plasseres i den politiske diskurs. Det er viktig å få fram at også private selskaper har påvirkningskraft i forhold til sikkerhetisering av cyberterrorisme, men det er det imidlertid ikke rom for å utdype videre i denne oppgaven.

6.2.7 Begrepsbruk/Nøkkelord

Mange av forskerne i utvalget er opptatt av begrepet krig (informasjonskrigføring og cyberkrig) i relasjon til cyberterrorisme. Jeg vil påpeke at krig er ikke sentralt for cyberterrorisme generelt ettersom det er stor forskjell på krig og terrorisme. Cyberterrorismebegrepet, slik det har utviklet seg og slik det framstilles av mange forskere og i media, ser ut til å gå mer i retning av kriminalitet enn av krigføring. Jeg velger likevel å ta med noen eksempler på akademikere som er opptatt av krigsbegreper i denne sammenheng, særlig fordi det har vært en del uklarheter knyttet til definisjoner av cyberterrorisme og relaterte begreper (se kap.4).

Når det gjelder begrepsbruk og nøkkelord i det akademiske nivå snakker Vatis (1998) om cybervåpen brukt av terrorister, og at det er det økende antall tilgjengelige *mål* som viser at trusselen er økende, men han bruker ikke ordet *cyberterrorisme*. Khalilzad (1999) bruker ikke ordet cyberterrorisme, men snakker om terrorisme og terrorister som farlige og utfordrende aktører. Han er opptatt av begreper som aktør, angrep og infrastruktur, og disse kan kalles hans nøkkelord.

Libicki er en av akademikerne som er mer opptatt av begrepet *krigføring* framfor *terrorisme*, og nevner derfor ikke cyberterrorisme, men derimot informasjonskrig, cyberkrig og hackerkrig. Det er vanskelig å nevne ett nøkkelord, det må i så fall bli informasjonskrigføring, for det er ulike typer av denne krigføringen han er opptatt av å skille fra hverandre i *What is Information Warfare* (1995).

Denning og O'Brien er de av forskerne i mitt utvalg som tydeligst er opptatt av og benytter begrepet *cyberterrorisme*. Rathmell (1997) bruker cyberterrorisme i overskriften på artikkelen, men skriver om informasjonskrigføring. Det som er spesielt med Rathmells artikkel, er at han bruker "cyberterrorisme" i overskriften og i innledningen, men videre skriver han om "informasjonskrigføring" før han mot slutten igjen nevner "cyberterrorisme". Dette er et interessant aspekt i og med at jeg tidligere har hevdet at definisjonene er vage og at ordene brukes om hverandre. Her ser vi at en fremtredende forsker også gjør det. Ordet brukes på en dramatisk måte som blikkfang, og ved at Rathmell bruker ordet er han med på å sikkerhetisere begrepet.

CSIS (1998) bruker strategisk informasjonskrigføring som hovedbetegnelse på den nye trusselen for nasjonal forsvarspolitikk, men kutter av og til ut ordet "strategisk". Det er tydelig at de ser for seg informasjonskrigføring som en slags samlebetegnelse på ulike former for angrep som kan komme fra ulike kilder og ha ulike taktiske mål. Dessuten må det påpekes at tittelen på forskningsrapporten er "Cybercrime… Cyberterrorism…Cyberwarfare". Dette er en fengende tittel som brukes som blikkfang. I rapporten blir ikke ordet cyberterrorisme benyttet i særlig stor grad, og det er heller informasjonskrigføring som nevnes som sannsynlig at terrorister kan tenke seg å bruke.

6.3 Diskurs på politisk nivå

Diskursen rundt begrepet cyberterrorisme ser ut til å vekke større interesse i den akademiske konteksten enn den politiske. Det har vært lettere å finne dokumenter hvor cyberterrorisme omtales i akademia enn i politikken. Diskursen på det politiske nivå er utvilsomt preget av farene knyttet til terrorisme, og mange tiltak er iverksatt for å redusere truslene, spesielt etter 11.september 2001. Avhengigheten av datateknologi har også ført til en levende diskurs rundt temaet "cybercrime", ofte kalt

datakriminalitet på norsk. De offisielle dokumentene gjenspeiler imidlertid lite fokus på cyberterrorisme som begrep, men jeg henviser til de kildene som "kommer nærmest" en diskurs om cyberterrorisme, se for øvrig 6.3.7 om begrepsbruk/nøkkelord. Kildene som benyttes er norske, amerikanske, fra Europarådet og EU-kommisjonen. Jeg ser på samme momenter i diskursen i dette delkapittelet som i det foregående.

6.3.1 Hva er trusselen?

Sårbarhetsutvalget skriver en del om hvilke sikkerhetsutfordringer samfunnet står overfor (NOU 2000:24): "Når det gjelder bevisste handlinger (for eksempel sabotasje eller terrorisme), er trusselbildet preget av en forskyvning fra det manuelle mot det elektroniske. De store endringene i bruken av informasjons- og kommunikasjonsteknologi endrer betydningen av landegrensene i sikkerhets- og beredskapssammenheng. Fremveksten av andre mulige motstandere enn nasjonalstater er nok et viktig utviklingstrekk." Når det gjelder risikoen for terror og sabotasje mot kritisk infrastruktur ser man for seg at bruk av datanettverk og EMP-våpen kan være sannsynlig.

St.meld.nr.17 (2001-2002) omtaler hvilke aktører man må ta hensyn til i samfunnssikkerhetsarbeidet framover. Også andre aktører enn de statlige kan gjøre stor skade på samfunnet, og man må derfor ta trusselen for terrorisme og organisert kriminalitet på alvor. I et avsnitt om terrorisme (St.meld.nr.17 (2001-2002): punkt 5.2.2) står det: "Terroristgrupper vil kunne foreta tre hovedtyper angrep: aksjoner med konvensjonelle våpen, aksjoner med masseødeleggelsesmidler og informasjonsangrep." Videre står det at "angrep på informasjonssystemer kan skje logisk (f.eks. datavirus) eller fysisk. Vestlige samfunns økende avhengighet av sårbare informasjonssystemer har skapt frykt for slike angrep, selv om det så langt finnes svært få eksempler på alvorlig cyber-terrorisme". Terrorisme ses med andre ord på som en trussel, men cyberterrorisme er ikke en uttalt trussel i seg selv.

Allerede på slutten av 1990-tallet ble cyberangrep uttalt som en erklært trussel fra amerikanske myndigheter under Bill Clintons presidentperiode. Cyberangrep kan komme fra internasjonale terroristgrupper eller agenter fra fremmede stater, men beskyttelse av den kritiske infrastrukturen, som er definert som sårbar, betyr også å kjempe mot lavskala-cyberangrep fra hackere (Reno 1998). Cyberangrep skaper spesielle problemer ved at angrepene gir "flytende" bevis, og angrepene kan komme fra hvor som helst i verden – cybertruslene overskrider vanlige grenser.

Det finnes mange synspunkter på terrorister og deres forhold til IT. Mark Pollitt ved FBI drøfter hvordan terrorister kan utnytte sårbarheten ved datasystemer og sier: "Could these vulnerabilities be utilized by terrorist elements? Certainly. These risks are independent of motive or perpetrator. These risks are structural to the use of computers" (Pollitt 2000). Han mener at risikoen er uavhengig av motiv, men det kan diskuteres om det er slik. Terrorister som angriper eller bruker datateknologi i sine angrep har som regel politiske og/eller religiøse hensikter.

Det er etablert en rekke ordninger og lover i EU med den hensikt å bekjempe terrorisme. I følge dokumentene som utgis i EU-systemet og i Europarådet, samt søk på nettsidene, ser det ut til at det er tradisjonell terrorisme og datakriminalitet som anses som de største truslene. I mitt kildegrunnlag finner jeg ikke at disse nevner trusselen for cyberterrorisme spesielt. Dette funnet støttes i en studie av Johansen (2004: 28) som skriver at "trusler mot informasjons- og kommunikasjonssystemene har imidlertid ingen prominent posisjon, heller ikke innen EUs anti-terrorstrategi". Tiltakene er særlig knyttet til å begrense finansieringen av terrorvirksomhet og hindre terrorgruppers bevegelsesfrihet. Europarådet har utformet en rekke lover for å forhindre terrorisme. Kort tid etter terrorangrepene 11. september 2001 vedtok EU en handlingsplan for bekjempelse av terror som blant annet inkluderte en felles definisjon av terrorisme og innføring av en felles arrestordre for å unngå behovet for formelle utleveringsprosedyrer. De senere år har det også kommet mange flere tiltak og handlingsplaner, men det går utenfor denne oppgavens ramme å nevne alle. Ettersom jeg ikke finner dokumenter som er rettet direkte mot cyberterrorisme er det

grunn til å anta at det skyldes at trusselen for tradisjonell terrorisme anses som større. Det gjøres imidlertid grundig arbeid innenfor ”cybercrime”-trusselen i EU, dette må dermed fremstå som en trussel. I følge et faktadokumentet om datakriminalitet fra Europarådet kommer de daglige truslene kommer fra spams, virus, hacking, identitetstyver og barnemishandling. Cyberterrorisme nevnes som en potensiell trussel for de sårbare samfunnene som er totalt avhengige av Internett (se The Council of Europe and Cybercrime). Europarådet vedtok en ”Convention on Cybercrime” i 2001 (som trådte i kraft 1. juli 2004) som er et bevis på at datakriminalitet tas på alvor ettersom det er den eneste bindende internasjonale dokument på området. Det danner retningslinjer for ethvert land som skal utvikle nasjonal lovgivning mot datakriminalitet og en ramme for internasjonalt samarbeid mellom statene som er med i traktaten.

6.3.2 Hvorfor finnes trusselen?

De fleste kildene som brukes i oppgaven beskriver teknologisk utvikling som den viktigste årsaken til at vi har fått samfunn med kritiske infrastrukturer som trues av de nye aktørene og midlene informasjonssamfunnet skaper. I følge NOU 2000:24 har teknologisk utvikling og framskritt ført til en grunnleggende omstrukturering av hele samfunnet. Teknologien fører til større effektivitet og gir åpnere samfunn med økt innsikt og tilgjengelighet. Samtidig har utviklingen innen data- og informasjonssystemer ført til stor gjensidig avhengighet og dermed større grad av sårbarhet, mellom de viktigste og mest kritiske samfunnsfunksjonene. Den teknologiske utviklingen fører til at flere aktører, både statlige og ikke-statlige, vil ha potensiale til å angripe og skade de viktige infrastrukturene (St.meld.nr.17 (2001-2002)).

I de fleste politiske dokumentene som er gjenomgått i denne analysen kommer det fram at trusselen fra hackere, cyberterrorister, stater med potensielt uhederlige motiver, eller hva det måtte være, skyldes utviklingen av globale nettverk som vi har gjort oss svært avhengige av. ”Our systems are more vulnerable than ever to attack

because of our unprededecedented reliance on technology", sa daværende justisminister Reno i forbindelse med opprettelsen av National Infrastructure Protection Centre ved FBI (Reno 1998). Energisystemer, transportnettverk og telekommunikasjonssystemer er mer sårbare enn noen gang fordi vi stoler på teknologi mer enn noen gang før (ibid.). I Clinton-administrasjonens Presidential Decision Directive 63 slås det også fast at trusselen finnes fordi USA er økende avhengig av enkelte kritiske infrastrukturer og cyber-baserte informasjonssystemer (White Paper 1998). Tradisjonelt har nasjonens kritiske infrastrukturer vært fysisk og logisk separert, men framskrittene innen informasjonsteknologi og behovene for økt effektivitet har ført til at disse infrastrukturene har blitt samkjørte og automatiserte. Framskrittene har også ført til nye sårbarheter i forhold til utstyrsfeil, menneskelig svikt, naturendringer og fysiske- og cyberangrep. Dokumentet framhever også at det er på grunn av USAs militære styrke at framtidige fiender, det være seg nasjoner, grupper eller individer, kan komme til å skade landet på utradisjonelt vis, inkludert angrep innenfor USAs territorium (ibid.).

I følge Europarådet skaper også vår avhengigheten av Internett sårbare samfunn. Ny informasjons- og kommunikasjonsteknologi gir føde til organiserte kriminelle som får nye verktøy å bruke for å utføre både tradisjonell kriminalitet og nye typer kriminalitet (se The Council of Europe and Cybercrime). Internett gjør det lettere for kriminelle å jobbe anonymt samt at det gir store muligheter for å danne nettverk med andre kriminelle. EU-kommisjonen slår videre fast at utviklingen av informasjons- og kommunikasjonssamfunnet har ført til behov for å sikre informasjonsinfrastrukturene og bekjempe datarelatert kriminalitet (KOMM 2000/890).

Sårbarhetsutvalget har slått fast "en gang for alle" at også Norge er et sårbart samfunn som følge av datateknologiens utvikling og vår avhengighet av denne. Denne sårbarheten skaper grobunn for en rekke nye trusselaktører og utvikling av midler både nye og tradisjonelle terrorister kan tenkes å utnytte.

6.3.3 Vurdering av trusselen

Sårbarhetsutvalget jobbet med ulike aspekter knyttet til IT, trusler, aktører m.m. og kom med ulike vurderinger knyttet det nye, såkalte "sårbare samfunn". Resultatet av Sårbarhetsutvalgets arbeid ble en rapport som kom ut som en norsk offentlig utredning (NOU). Problemet med et dokument som *NOU 2000:24 – Et sårbart samfunn* er at det er et politisk-administrativt dokument gitt ut under Justisdepartementet, men bidragene i utredningen er basert på ulike kilder, blant annet svært mange forskeres synspunkter. Forskernes synspunkter har jeg valgt å plassere på akademisk nivå, men siden de i denne forbindelse har utarbeidet rapporter på *oppdrag* fra Sårbarhetsutvalget, velger jeg å analysere utredningen på politisk nivå og nevner ikke spesifikt hvem som har kommet med bidragene jeg refererer til[35]. Sårbarhetsutvalget har valgt ut deler av bidragene de har fått av f.eks. forskere, og når det står i utredningen må man regne med at det er synspunkter også utvalget vil stå inne for. Det ser ut til å være en utbredt oppfatning at den teknologiske utviklingen påvirker samfunnssikkerheten og at vi er blitt avhengige av informasjons- og kommunikasjonssystemer. Det står blant annet: "Med forholdsvis enkle midler er det i dag mulig å lamme viktige virksomheter og samfunnsfunksjoner gjennom fiendtlige informasjonsoperasjoner. Risikoen for et ødeleggende elektronisk angrep er på mange måter like reell som et mer konvensjonelt militært angrep" (NOU 2000:24:s.37). Et interessant diskusjonstema er hvorvidt terrorister faktisk vil komme til å gjennomføre terroraksjoner mot datamål og kritisk infrastruktur i stedet for tradisjonelle mål. "Så langt vet man lite om terrorgruppers interesse for bruk av IKT som terrorvåpen eller terrormål" (NOU 2000:24:s.40). Flere steder i utredningen står det at det ikke er rapportert om organiserte og alvorlige dataangrep (ibid.:37, 40).

Nærings- og handelsdepartementet har gitt ut en rapport, "Samfunnets sårbarhet som følge av avhengighet til IT", hvor det også legges vekt på fordeler og ulemper ved

---

[35] Se Sårbarhetsutvalgets rapport (NOU 2000:24) hvor kildene er nevnt spesifikt i de fleste kapitler.

IKT slik som i NOU 2000:24. Rapporten er utarbeidet av et IT-sårbarhetsprosjekt, med styringsgruppe og prosjektgruppe med representanter fra ulike departementer, som også har koordinert sitt arbeid med Sårbarhetsutvalgets arbeid innenfor samme område. Når det gjelder trusselvurderinger står det i rapporten: ”Frem til i dag har svikt i IKT-systemer i hovedsak hatt årsak i enten tilfeldige ikke-villede hendelser eller ustrukturerte angrep fra enkeltindivider. De mest strukturerte angrepene synes så langt å ha dreiet seg om ulike former for vinningsforbrytelser”(NH-dep. 2000:21). Det synes som rapporten ikke bærer preg av konkrete konklusjoner vedrørende vurderinger ev fremtidige trusler og trusselnivå mot IKT-systemer og infrastrukturer i samfunnet. Det blir hevdet at trusselvurderingene er forbundet med stor usikkerhet.

I Forsvarets fellesoperative doktrine, del B, finnes det et kapittel som omhandler *Informasjonsoperasjoner*. Doktrinen er mer opptatt av håndteringen av konflikt og prinsipp for bruk av militærmakt framfor trusselvurderinger, men deres behandling av og syn på informasjonsoperasjoner er likevel et interessant bidrag til diskursen. NATO har lagt seg på en linje hvor informasjonsoperasjoner har blitt en stadig viktigere del av det strategiske nivå. Det gjenspeiles også i dokumenter som *MC 422 NATO Information Operations (INFO OPS)* fra 1998 som viser at informasjonsoperasjoner lenge har vært et uttalt viktig konsept innen NATO. Informasjonsoperasjoner som omfatter både militære og sivile tiltak/virkemidler og som har både en defensiv og offensiv side har også blitt en viktig del av den norske militære doktrine. De avanserte kommunikasjons- og informasjonssystemene som finnes i den sivile og militære kommandokjeden er sårbare overfor informasjonsoperasjoner (FFD, del B, 2000:71). Den databaserte tidsalderen har skapt nye trusler og utfordringer for det militære og med vektlegging av informasjonsoperasjoner i den fellesoperative doktrine ser det ut til at de nye truslene blir tatt på alvor og at nye strategier er under utforming.

Frykten for samfunnets økende sårbarhet og hvilke muligheter det gir nye aktører er uttalt i Stortingsmelding nr 22 (1997-98): *Hovedretningslinjer for Forsvarets*

virksomhet og utvikling i tiden 1999-2000: ”Samfunnets økende avhengighet av informasjonssystemer og utviklingen mot åpne, verdensomspennende datanettverk har også skapt sårbarhet på sivil side. Sårbare systemer kan rammes av både sivile og militære aktører som ønsker å skape frykt, ødeleggelse eller kaos i samfunnet” (St.meld.nr.22 (1997-98): boks 4.1). Videre skriver de: ”I verste fall kreves det bare kunnskap og en datamaskin med tilkoplet modem for å spre desinformasjon eller plante datavirus i systemer som fysisk befinner seg på den andre siden av jordkloden” (ibid.).

I en tale på en konferanse om beskyttelse av kritisk infrastruktur uttalte den tidligere amerikanske justisministeren, Janet Reno, at ”our systems are more vulnerable than ever to attack because of our unprecedented reliance on technology” (Det amerikanske justisdepartementet 1998). I talen annonserte hun opprettelsen av National Protection Center (NIPC) ved FBI. ”The NIPC’s mission is to detect, to prevent and to respond to cyber and physical attacks on our nation’s critical infrastructures and to oversee FBI computer crime investigations conducted in the field” (Reno 1998:12). Videre hevder Reno at ”Cyber attacks pose unique challenges. Because of the technological advancements, today’s criminals can be more nimble and more elusive than ever before” (Reno 1998:19). I tillegg kommer hun med utsagn som: ”Cyber attacks create a special problem, because the evidence is fleeting” og ”Cyber threats ignore the borders. The attack can come from anywhere in the world” (ibid.). Uttalelsene gir grunn for å anta at cybertruslene ble ansett som så store at NIPC ble opprettet som et tiltak for å prøve å redusere trusselen.

På våren i 1998 utga Clinton-administrasjonen et White Paper (Presidential Decision Directive 63) med nøkkelelementer fra administrasjonens policy på beskyttelse av kritisk infrastruktur. Målet var å spre det til alle interesserte parter både i offentlig og privat sektor. I dokumentet legges det vekt på at USA er økende avhengig av kritiske infrastrukturer og cyber-baserte informasjonssystemer. Som en supermakt innen

økonomi og militær makt er landet i økende grad sårbart og det er presidentens intensjon å sikre kontinuiteten i infrastrukturen (White Paper 1998).

EU vurderer sikkerhetsutfordringene som store som følge av at kommunikasjon og informasjon er blitt en nøkkelfaktor i den økonomiske og samfunnsmessige utviklingen (KOMM 2001/298). Europarådets konvensjon om "cybercrime" kan tolkes dit hen at vurderingene går i retning av at datakriminalitet ses på som en mer reell og større trussel enn cyberterrorisme blant de europeiske land. Europarådets aktiviteter i kampen mot terrorisme er knyttet til tre grunnpilarer: styrke rettslige skritt mot terrorisme, beskytte fundamentale verdier og finne årsakene til terrorisme. Cyberterrorisme blir ikke nevnt spesifikt som en konkret og reell trussel. Det samme gjelder for EU-kommisjonen og Rådet for den europeiske union (Ministerrådet) som har gitt uttalelser og innført lover i kampen mot terror og datakriminalitet, men uten av cyberterrorisme nevnes spesifikt.

6.3.4 Konsekvenser

Sårbarhetsutvalget vektlegger farene IKT-systemene[36] kan bli utsatt for som angrep i datasystemer ved hjelp av hacking og virus for å stjele, manipulere og ødelegge data. Slike angrep kan få alvorlige økonomiske konsekvenser. "I tillegg gir den nye teknologien muligheter til å gjennomføre angrep som er politisk, militært eller sosialt motivert. Alvorligst er risikoen for informasjonsoperasjoner fra stater eller store terrorgrupper" (NOU 2000:24:s.37). Det antas med andre ord at terrorister utgjør en stor trussel.

Ettersom EU er mer opptatt av datakriminalitet enn cyberterrorisme blir beskrivelsene av konsekvenser deretter. I en meddelelse fra EU-kommisjonen beskrives en rekke uheldige konsekvenser av uhell og ondsinnede handlinger rettet mot et

[36] IKT: Informasjons- og kommunikasjonsteknologi.

informasjonssystem som f.eks. uautorisert inntrengning i datamaskiner, virus, forfalskning av identitet m.m. Det foreslås videre tiltak for å redusere disse eventuelle konsekvensene. Her er vi imidlertid litt på siden av det som er tema, selv om terrorisme absolutt kan knyttes til kriminalitet. Det er med andre ord ikke funnet EU-dokumenter som beskriver konsekvenser av cyberterrorisme.

Konsekvenser av cybertrusler, eventuelt cyberterrorisme, er i stor grad knyttet til sammenbrudd av kritiske infrastrukturer. I følge "The Cyber Security Information Act" som ble introdusert i USA i 2001 kan et cyberangrep raskt lamme én eller flere kritiske infrastrukturer samtidig (se Congressional Bill 2001). Det er ikke lenger bare tenåringer som utfører cyberangrep, men er i ferd med å læres og bli brukt av terrororganisasjoner. Privat sektor har kommet lenger enn offentlig sektor angående informasjon om cybertrusler og sårbarhet. Loven ble introdusert for å øke samarbeidet mellom industrier og mellom privat og offentlig sektor på dette området.

6.3.5 Framtidsperspektiv

Det var et mål å finne eksempler på klare uttalelser vedrørende når man tror cyberangrep fra terrorister vil komme, hvor vanlig det kommer til å bli o.l.., men diskursen knyttet til framtidsperspektiver er heller preget av generelle antydninger hvor særlig interesser og virkemidler står i sentrum. Det er kjent at terroristgrupper bruker Internett for propaganda og kommunikasjon, men man vet lite om hvor interessert de er i å bruke informasjonsteknologi som våpen og om de har interesse av å angripe informasjonsteknologi. Tidligere har det ikke vært vanlig at terrorister har angrepet infrastruktur, og årsaken til det kan være at tradisjonelle former for terrorisme, gjerne med bruk av bomber, er mer spektakulære og gir større medieoppmerksomhet (NOU 2000:24:s.40). Nærings- og handelsdepartementets rapport vektlegger at nye aktører kan komme på banen, kanskje raskere enn vi kan tenke oss, og det er derfor nødvendig med tiltak for å beskytte oss mot mulige trusler. På den ene siden blir det hevdet at "eksisterende terroristorganisasjoner i liten grad

kan forventes å ta i bruk denne typen virkemidler, men i stedet velger å holde seg til velkjente virkemidler", men en annen vurdering "som er mye fremme i den offentlige debatten på området er at også tradisjonelle organisasjoner med tiden vil ta i bruk hele spennet av virkemidler"(NH-dep. 2000:24).

Framtidsperspektivene er knyttet til scenarier, og de er det mange av i forbindelse med cyberterrorismebegrepet! Internett gir grobunn for mange potensielle trusler, og det er her trusselen for cyberterrorisme kan plasseres. Ettersom truslene for cyberterrorisme er potensielle, men foreløpig ikke reelle ettersom det ikke har funnet sted cyberterroristangrep, er det kanskje naturlig at det står skrevet mer om framtidsutsikter knyttet til dette begrepet i akademia enn i politiske dokumenter. De mange tiltakene i form av handlingsplaner og lover som har blitt iverksatt i USA og i EU-systemet, særlig i perioden fra 11.september og fram til i dag, er imidlertid tegn på at terrorisme generelt er en trussel som tas på alvor i stadig større grad. Og det til tross for at antallet ofre for internasjonal terrorisme er svært lav målt mot de fleste former for organisert voldsutøvelse nasjonalt og internasjonalt (Johansen 2004:25). Det er potensialet for terrorisme som gjør at trusselen for terrorisme generelt ses på som stor i framtida og at det derfor iverksettes tiltak for å forhindre angrep.

6.3.6 Mediediskurs

En god del av avisartiklene som omhandler cyberteknologi dreier seg om hacking, som f.eks. hackere som har brutt seg inn i Microsoft og hackere som har modifisert eller lagt ned yahoo.com o.l.. Computerworld skriver blant annet at i Norge bygger Politiets overvåkingstjeneste (POT)[37] en enhet mot "kyberterror" som skal bekjempe datakriminalitet og cyberterrorisme som kan skade rikets sikkerhet (Heggelund 1999). I følge Computerworld hevdet daværende overvåkingssjef Per Sefland at

[37] Nåværende Politiets sikkerhetstjeneste (PST).

”datakriminalitet og cyberterrorisme skjer nå oftere på bekostning av rikets sikkerhet” (ibid.). En anonym kilde fra Overvåkningspolitiet sier at ”det norske samfunnet er blitt så informasjonsavhengig, at det bare er et tidsspørsmål før noen går inn og destabiliserer det med cyberterrorisme eller datakriminalitet som våpen. Norge har allerede vært utsatt for cyberterrorangrep, men disse har foreløpig ikke vært så alvorlige eller hatt store ringsvirkninger” (ibid.). Disse utsagnene viser at politiet tar dataterrorismetrusselen alvorlig og er med på å sikkerhetisere ved blant annet å knytte cyberterrorisme til rikets sikkerhet. Jeg har imidlertid ikke funnet at det finnes en ”enhet mot kyberterror” som omtales ovenfor; det kan være at det siktes til det som i dag er Politiets datakrimsenter og som ligger under Kripos.

I norske medier har det de senere år vært mange oppslag i mediene knyttet til dataterrorisme og om Norge er forberedt på dette. Allerede da Sårbarhetsutvalget utga sin rapport i 2000 ble det skrevet mye om hvordan Norge bør og kan møte den nye elektroniske trusselen. I et oppslag i VG i 2001 hevdet Jan Erik Larsen, lederen for daværende Sikkerhetsstaben i Forsvarets Overkommando, at Norge ikke har et nasjonalt forsvar mot angrep via nettet og at det er behov for at dette må forbedres kraftig (VG-nett 2001). Videre hevdet han at elektroniske angrep er langt verre enn stridsvogner på grensen. Tre år senere er Larsen direktør i Nasjonal sikkerhetsmyndighet (NSM) og uttaler at ”før eller siden vil det komme et større, målrettet dataangrep mot den kritiske infrastrukturen i Norge. Det er bare et spørsmål om tid” (Aftenposten 2004). Norske databedrifter angripes daglig av hackere, og myndighetene frykter at terroristorganisasjoner vil bruke datamaskiner for å lamme økonomien i vestlige land (ibid.). Senere etterlyser hans kollega, Cristophe Birkeland, leder av VDI-systemet[38] i NSM et sikkerhetsorgan mot cyberterrorisme i Norge (Nettavisen 2005).

[38] VDI: Varslingssystem for digital infrastruktur.

I en uttalelse til BBC News i forbindelse med innføring av ny anti-terrorismelovgivning i Storbritannia (”The Terrorism Act”), snakket innenriksminister Jack Straw samtidig om trusselen for cyberterrorisme (BBC News 2001). Straw hevdet at resultatene av cyberterrorisme (ved at noen f.eks. hacker seg inn på kontrollsystemene til vann- og kraftforsyningsanlegg) kan få større følger enn de direkte følgene av en eksplosjon, og det har derfor vært nødvendig å inkludere dette i loven (ibid.). Dette er ett av få eksempler eksempler jeg har funnet på at ministre uttaler seg om og bruker begrepet cyberterrorisme, dette var til og med før terrorhendelsene 11.september 2001.

I en reportasje i USA Today 11.06.98 uttrykte lovgivere og personell i Clinton-administrasjonen frykt for cyberterrorisme. Richard Clarke, sikkerhetspolitiker og sjef for National Security Council, sa:”…if steps aren’t taken, enemy nations, terrorists or criminal cartels could try to cripple this country by disrupting banking and finance, creating widespread power outages, interrupting transportation systems and crashing communications networks” (USA Today 1998). I en artikkel på CNN Norge (2000) uttaler dataeksperter at USA er sårbart for elektroniske snikangrep og at de frykter Pearl Harbor i cyberspace. I artikkelen siteres den ovennevnte Richard Clarke som sier at ”utenlandske ”cyber-krigere” er en reell trussel mot landets sikkerhet” og påpeker at ”en rekke nasjoner har opprettet sine egne avdelinger for krigføring i cyberspace” (CNN Norge 2000). Videre uttaler han at ”en krig i cyberspace eller store forstyrrelser av kyberrommet er verken uunngåelig eller overveiende sannsynlig. Men begge deler er mulig, og derfor bør vi også beskytte oss mot denne muligheten, før vi rammes av et digitalt Pearl Harbor eller dataverdenens ”Exxon Valdez”” (ibid.). IT-avisen (2000) skriver: ”Neste krig kommer på nett – USA forberedt på ”cyber-terror” og fortsetter med en kommentar fra lederen for USAs topphemmelige National Security Agency: ”Nettet blir en av fremtidens viktigste krigsskueplasser”. Disse bidragene viser hvordan sjefen i det amerikanske sikkerhetsrådet har uttalt seg i en mediekontekst. Her brukes ord som terrorister, cyberterrorisme og cyber-krigere. Det kan skyldes at media gjengir intervjuet med ord som skal fungere som blikkfang på

leseren, og slik øker graden av sikkerhetisering av begrepet cyberterrorisme. I tillegg er det også sannsynlig at Clarke, og andre i tilsvarende posisjoner, uttaler seg på en annen måte til pressen i et intervju enn i skriftlige, faglige dokumenter. BBC News (2000) skriver også om cybertrusselen, men gjengir blant annet uttalelsene fra en som er *skeptisk* til cyberterrorisme. Kevin Poulsen, som jobber for Security Focus.com, mener at informasjonssystemer har blitt mer, ikke mindre, sikre over tid og forkaster ideen om et elektronisk Pearl Harbor som ofte blir brukt i informasjonskrigføringssirkler. ”We don’t need to invent an enemy to protect our networks”, var hans avsluttende kommentar (ibid.).

6.3.7 Begrepsbruk/nøkkelord

Som nevnt innledningsvis i dette delkapittelet er det få dokumenter i den politiske diskursen som har cyberterrorisme som nøkkelord, så her vil det også komme inn nøkkelord knyttet til krig som i 6.2.7, men også kriminalitet som er mer beslektet med cyberterrorisme enn krigføring.

Når det gjelder definisjon på informasjonskrigføring i Stortingsmelding nr. 22 står det: ”Informasjonskrigføring er angrep på og forsvar av informasjon og tilhørende systemer. I militær forstand omfatter slik krigføring angrep av både fysisk, psykologisk og elektronisk art”(St.meld.nr.22 (1997-98): boks 4.1). Forsvarsdepartementet bruker her begrepet *informasjonskrigføring* i stedet for *informasjonsoperasjoner* som har blitt mer vanlig innen Forsvaret siden stortingsmeldingen ble skrevet, og det viser at begrepsutviklingen ikke hadde kommet spesielt langt på det tidspunktet meldingen ble skrevet. Definisjonen er vag og inneholder ikke om hva som er sårbart, hva som blir utsatt for en trussel og hva som kan bli angrepet (bortsett fra ”informasjon og tilhørende systemer” som ikke er særlig konkret). Det er likevel tydelig at man vil understreke hvilken betydning og påvirkning den økte bruken av informasjonsteknologi har på samfunnet. I St.meld.nr.17 (2001-2002) er det et avsnitt om utviklingen i risiko- og trusselbildet i

samfunnet hvor det skrives om både truslene for terrorisme og organisert kriminalitet. Cyberterrorismebegrepet blir nevnt, men ikke omtalt i vesentlig grad.

I Europa, både innenfor EU-systemet og i Europarådet brukes begrepet cyberterrorisme i liten grad, det er terrorisme og "cybercrime" som kan regnes som nøkkelord her. Et nyhetssøk på Europarådets nettside[39] (fra og med 01.11.00) viser at ingen treff kommer opp ved å taste inn "cyberterrorism", men det kommer opp 67 treff relatert til "cybercrime" og 353 treff på "terrorism". Søk på EU-kommisjonens og Rådet for den europeiske unions nettsider viser heller ingen treff på cyberterrorisme. Dette er i samsvar med dokumenter som er utgitt fra Europarådet og Kommisjonen; konvensjoner og meddelelser ("communications"), som i stor grad dreier seg om "cybercrime", beskyttelse av kritisk infrastruktur i forbindelse med terrorisme, bekjempelse av terrorisme m.m.framfor dokumenter om cyberterrorisme. På Europarådets nettside fant jeg imidlertid et faktadokument om Europarådet og "cybercrime"[40], og som tittelen indikerer er "cybercrime" nøkkelordet, men her nevnes faktisk cyberterrorisme som en potensiell trussel.

I det amerikanske kildegrunnlaget er "cybertrusler" og "cyberangrep" nøkkelord, og kritisk infrastruktur er det som blir omtalt som det som er sårbart og kan bli utsatt for slike trusler og angrep fra "cyberspace" (se feks Congressional Bill 2001; Department of Homeland Security 2003). Cyberterrorismebegrepet er svært sentralt i amerikansk akademisk litteratur, og en av de fremste forskerne på området, Dorothy Denning har blant annet talt til Representantenes hus om temaet i 2000 (Denning 2000b). De politiske dokumentene i mitt utvalg har derimot ikke cyberterrorisme som hovedfokus, men omtaler altså cybertrusselen som svært stor og sannsynlig som det må iverksettes tiltak for å bekjempe.

---

[39] www.coe.int

[40] www.coe.int/cybercrime

6.4 Har cyberterrorisme blitt sikkerhetisert?

På bakgrunn av foregående analyser er det betimelig å gå tilbake til problemstillingen og spørre om cyberterrorisme kan sies å ha blitt sikkerhetisert? Tidligere, under punktet om sikkerhetisering i teorikapittelet, blir det sagt at en sak blir sikkerhetisert når den blir presentert som en eksistensiell trussel som legitimt krever spesielle tiltak som går utenfor vanlige politiske prosedyrer. Jeg må se på om disse kriteriene er oppfylt for å si om en sak (her: cyberterrorisme) har blitt sikkerhetisert, men det kan imidlertid være vanskelig å se hva som regnes som ”spesielle tiltak”. Tiltak som lovgivning kan defineres som ekstraordinære, det er mer uklart om handlingsplaner og andre lignende tiltak kan regnes som tiltak som beviser at en sikkerhetisering har funnet sted. Sistnevnte tiltak kan imidlertid regnes som sikkerhetiserende handlinger.

6.4.1 Sikkerhetiserende handlinger og sikkerhetisering

Talehandlingene som er framstilt både i dette og forrige kapittel viser hvordan de sikkerhetiserende aktørene på akademisk og politisk nivå (og delvis i media) snakker om begrepet cyberterrorisme og relaterte begreper. Svaret på problemstillingen må nødvendigvis søkes besvart ved å se på sikkerhetisering på politisk nivå ettersom det kun er politikere som kan fullstendig sikkerhetisere ved å iverksette ekstraordinære tiltak. Forskernes (og delvis journalisters)”speech acts” i kapittel 5 og 6 er bevis på at de er deltakere i sikkerhetiseringsprosessen, men de kan i følge teorien bare komme med nettopp ”speech acts” og ikke være med på å sikkerhetisere. Med andre ord, de deltar i en sikkerhetiseringsprosess hvor deres ”speech acts” kun er sikkerhetiserende handlinger. Jeg vil påstå at akademikerne er med på å gjøre cyberterrorisme til et sikkerhetsanliggende ved sine talehandlinger. De er med på å framstille cyberterrorisme som en potensiell trussel, mange forskere forsøker å grunngi hvorfor, og de beskriver hvilke midler de kan tenkes å bruke og hvilke hensikter de kan ha ved å gå til slike angrep.

Når det gjelder politisk nivå har jeg forsøkt å finne ytringer og skriftlige formuleringer som viser om og eventuelt hvordan de politiske sikkerhetiserende aktørene konkret er med på å sikkerhetisere. Delkapittel 6.3 viste sikkerhetiseringsdiskursen blant disse aktørene, og nedenfor følger et komprimert utvalg eksempler på sikkerhetisering innen den politiske kontekst. Det er viktig å påpeke at selv om det er eksempler på at cyberterrorisme har blitt sikkerhetisert, er det ikke nødvendigvis snakk om fullstendig sikkerhetisering. Det kommer jeg tilbake til nedenfor, se 6.4.3.

Forfatterne av Sårbarhetsutvalgets rapport er med på å gjøre en sak til et sikkerhetsanliggende ved å skrive at både statlige og ikke-statlige aktører (potensielt cyberterrorister selv om ordet ikke brukes) har midler til å angripe informasjons- og kommunikasjonssystemer og at de dermed utgjør en trussel. Ordet cyberterrorisme blir ikke brukt i Nærings- og handelsdepartementets rapport (2000), men det er en uttalt, om enn nyansert, fare og trussel ved at terrorister kan komme til å bruke nye virkemidler mot nye typer mål i framtida. Vi har her eksempel på en talehandling hvor cyberterrorisme, indirekte, blir sett på som en trussel, og blir dermed gjort til en sikkerhetssak. Forsvarets fellesoperative doktrine, del B (2000) preges ikke av trusselvurderinger, men mer konkrete opplysninger om strategier og målsettinger i forsvaret. Det er derfor vanskelig å finne mer konkrete eksempler på sikkerhetisering enn at man oppfatter at de nye truslene tas på alvor. Teknologien gir både nye muligheter og nye utfordringer og mange sektorer i samfunnet er etter hvert svært avhengige av at datasystemene fungerer. ”Selv om disse utviklingstrekkene peker i retning av både større og mindre sårbarheter i samfunnet, *øker likevel samfunnets samlede sårbarhet*. Et komplekst og gjensidig avhengig samfunn er ikke sterkere enn sitt svakeste ledd. Uten tilstrekkelige sikkerhetsmekanismer kan de kritiske svakhetene utnyttes av så vel enkeltpersoner som velorganiserte grupper og statlige aktører”(St.meld.nr.22 (1997-98): punkt 4.5.2). Totalt sett viser disse uttalelsene at frykten for datateknologiens muligheter og sårbarheter er stor og at tiltak må settes inn for å møte den økende trusselen fra grupper og stater. Terrorister og cyberterrorister blir ikke nevnt konkret, men kan trolig inngå i ”velorganiserte

grupper". Gjennom denne Stortingsmeldingen deltar myndighetene i en sikkerhetiseringsprosess av trusselen for cyberterrorisme og informasjonskrigføring (eller informasjonsoperasjoner) på grunn av at samfunnets sårbarhet og truslene det skaper og gir blir omtalt på en slik måte at en slik påstand kan rettferdiggjøres.

Dokumentet MC 422 skal vise hvordan INFO OPS kan implementeres i NATO, og siden det er et mål, blir informasjonstrusselen tatt på alvor. I så måte bidrar NATO i sikkerhetiseringsprossen ved at trusselen mot bruken av IT i militære operasjoner og mot kritiske informasjonsstrukturer uttales. Informasjonsoperasjoner er her ment som en strategi for forsvaret i framtidige konflikter. Underforstått ligger tanken om informasjonsoperasjoner som en trussel også mot egen stat fordi andre stater kan tenkes å bruke den strategien mot en selv.

Uttalelsene fra Janet Reno (1998) som går på faren og utfordringene ved cyberangrep viser at den amerikanske stat tar cybertruslene alvorlig og bidrar til å gjøre dem til et sikkerhetsanliggende. Faren blir antatt som stor og dette bekreftes også i at det gjøres noe med cybertrusselen ettersom blant annet NIPC[41] ble etablert. Det settes i gang tiltak for å beskytte landet og stoppe eventuelle cyberangrep fordi faren og trusselen blir ansett som tilstedeværende. Her kan man konkludere med at det amerikanske justisdepartementet på vegne av den amerikanske stat har sikkerhetisert cyberterrorisme gjennom sin vektlegging av trusler kritisk infrastruktur står overfor. Clinton-administrasjonen sikkerhetiserte datatrusselen ved implementering av tiltak som skal beskytte infrastrukturen de anser som sårbar, og ved å ta initiativ til arbeidet som ledet fram mot opprettelsen av NIPC. En rekke organer og institusjoner med ansvar for nasjonens kritiske informasjonsinfrastrukturer ble etablert både under Clinton- og Bush-administrasjonen. Introduksjonen av en Cyber Security Act i 2001 er også bevis på sikkerhetisering. Siden det har blitt lagt stor vekt på *tiltak*, indikerer det at trusselen for angrep mot kritisk infrastruktur blir sett på som stor og alvorlig for USA.

6.4.2 Tiltak på politisk nivå

Flere av de sikkerhetiserende aktørene på politisk nivå er opptatt av tiltak for å redusere faren og minske trusselen for angrep rettet mot informasjonssystemer og kritiske infrastrukturer. Etableringen av disse tiltakene kan regnes som sikkerhetiserende handlinger og eksempler på at sikkerhetisering har funnet sted.

Det er nødvendig med internasjonale lover og reguleringer for å styre og kontrollere informasjonssamfunnet (Krutskikh 1999:34) og dermed om mulig hindre kriminell bruk av informasjon. Man må få internasjonalt samarbeid på utveksling av terrorismeinformasjon og samle det i et integrert system slik at det å møte terrorismetrusselen blir en internasjonal prioritet (Stewart 1987:251). I dagens internasjonale lovverk finnes nær sagt ingen reguleringer som kan begrense teknologiutviklingen og det den fører med seg; frykt for bruk av informasjonsteknologi mot kritiske informasjonssystemer (Votrin 1999). Siden informasjonssamfunnet mangler reguleringer kan informasjonsvåpen lett bli svært attraktive. Informasjonssikkerhet er en sak som berører hele det internasjonale samfunnet. Votrin avslutter med at vi trenger et framtidig internasjonalt legalt regime på informasjonssikkerhet. Alle land bør opprette samarbeidsorganisasjoner for å minske farene fra ”den nye terrorismen” (Lee 1999). Som nevnt tidligere vedtok Europarådet en ”Convention on Cybercrime” i 2001. Teksten er den første internasjonale traktaten som tar opp kriminallovgivning og prosedyremessige aspekter ved ulike typer misbruk av datasystemer, nettverk og data. Målet med konvensjonen er å harmonisere nasjonal lovgivning på dette området. Dette er et svært viktig tiltak og Europarådet (ved de europeiske statene som har ratifisert konvensjonen) viser med dette at de er med på å sikkerhetisere ”cybercrime”, og indirekte kanskje cyberterrorisme. En konvensjon er også et sterkt virkemiddel i forhold til andre mer ubindende overenskomster.

---

[41] NIPC: National Infrastructure Protection Centre.

EU har foretatt en rekke tiltak knyttet til å bekjempe ulovlig innhold på Internett. I 1999 innførte Europaparlamentet og Ministerrådet en "multiannual action plan" for å fremme sikrere bruk av Internett i kampen mot ulovlig innhold på de globale nettverkene. På Tampere toppmøtet i 1999 konkluderte Ministerrådet med at "high-tech crime" skulle inkluderes i felles definisjoner og sanksjoner. Jeg har tidligere vist til meddelelsen fra EU-kommisjonen om "Et sikrere informasjonssamfunn: Forbedring av sikkerheten i informasjonsinfrastrukturene og bekjempelse av datarelatert kriminalitet" som kom i januar 2001 (KOMM 2000/890). Meddelelsen var det første forsøket på å presentere en helhetlig policy –uttalelse om "cybercrime", og Kommisjonens ønske var å skape en deball på EU-nivå mellom alle interessentene. For å følge opp instruksjonene gitt av ministerne på toppmøtet i Tampere har EU-kommisjonen presentert forslag for en "Council framework decision" som skal danne tilnærming til en lov mot blant annet angrep mot informasjonssystemer (hacking, denial of service og virus). Forhandlinger om dette pågår fortsatt[42]. Disse tiltakene til Kommisjonen viser at datakriminalitet og usikkerheten det skaper, særlig i forhold til informasjonsinfrastrukturene, er en sikkerhetiserende handling fra EUs side, selv om ikke ordet cyberterrorisme blir brukt i denne sammenhengen.

I NOU 2000:24 drøftes nye utfordringer for samfunnet og samtidig foreslås sektorvise tiltak for økt samfunnssikkerhet, deriblant beskyttelse av IKT og kraftforsyning, transport, olje- og gass, vannforsyning m.m. Når det gjelder strategier for å redusere samfunnets IKT-sårbarhet, legges det vekt på informasjonsutveksling mellom det private og det offentlige, øke varslingsevnen til systemene i samfunnsmaskineriet, øke kompetanse, utdanning og forskning (danne nettverk), utvikle juridiske rammeverk i forhold til den teknologiske utviklingen, og etablere partnerskap mellom offentlige og private virksomheter (NOU 2000:24:s.70). St.meld.nr.17 (2001-2002) beskriver dagens trusselbilde som et mangfold av utfordringer som må møtes med et mangfold av tiltak, både forebyggende og konsekvensreduserende. Terrorangrepene 11.september skapte store endringer i trussel- og risikobildet, og samfunnet må være i

[42] http://ec.europa.eu/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm

stand til å møte en rekke utfordringer i tillegg til de tradisjonelle militære. Meldingen gir en oversikt og tilbakemelding på bakgrunn av Sårbarhetsutvalgets anbefalinger på en rekke sektorer. Det skal f.eks. etableres et senter for informasjonssikring for å møte utfordringer innen IKT-sektoren, beredskapen innen kraftforsyningen skal styrkes og transportberedskapen skal utredes. Meldingen viser også til tiltak som er gjennomført. Eksempelvis er beredskapen i forhold til masseødeleggelsesmidler skjerpet vesentlig etter terroraksjonene den 11. september 2001 og ytterligere tiltak vil bli vurdert. I etterkant av Europarådets Convention of Cybercrime som Norge undertegnet 23.11.01, ble det laget en NOU 2003: 27 *Lovtiltak mot datakriminalitet*. For at Norge skulle kunne ratifisere konvensjonen var det nødvendig med visse lovendringer. Datakrimutvalget ble etablert og fikk dermed mandat til å foreslå nødvendige lovtiltak for gjennomføring av Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi. Utvalget leverte overnevnte NOU med lovforslag som omfattet utkast til enkelte endringer i straffeloven og straffeprosessloven[43].

I Clinton-administrasjonens Presidential Decision Directive 63 skisseres nasjonale mål, samarbeid mellom offentlig og privat sektor for å redusere sårbarheten, retningslinjer for å øke sikkerheten, struktur og organisering av de instanser som har ansvar for å beskytte de ulike infrastrukturene, oppgaver som må gjøres for å fullføre den nasjonale infrastruktursikringsplanen, og plan for implementeringen av beslutningene (White Paper1998). Clinton-administrasjonen viste allerede i 1995 gjennom en Presidential Decision Directive 39 (PPD-39) at problemene rundt sårbar kritisk infrastruktur måtte settes på dagsordenen. Justisministeren ble satt til å lede en regjeringskomité som skulle vurdere sårbarheten til nasjonens kritiske infrastrukturer og anbefale tiltak for å beskytte dem (Vatis 1998). Ministeren dannet en Critical Infrastructure Working Group som skulle fokusere på trusler og sårbarheter. Som

[43] Delutredning II kom ved NOU 2007:2 *Lovtiltak mot datakriminalitet*. På grunn av den raske teknologiutviklingen i samfunnet er det behov for en straffelovgivning som fanger opp eksisterende og nye kriminalitetstrusler. Datakrimutvalget fant at dagens regler om datakriminalitet var utilstrekkelige og at det var behov for presiseringer og en viss nykriminalisering (NOU 2007:2).

nevnt ovenfor ble NIPC dannet i februar 1998 og i mai 1998 kom presidentens PPD-63 som formelt anerkjente NIPCs rolle innen regjeringens rammeverk for behandling av infrastrukturbeskyttelse (ibid.). En del av arbeidet Clinton startet innen dette området ble videreført av Bush-administrasjonen, særlig etter 11.september-angrepene. I november 2002 signerte George W. Bush en lov som førte til etableringen av Department of Homeland Security. Departementet utga i 2003 *The National Strategy to Secure Cyberspace* som en del av bestrebelsene på å beskytte nasjonen, og den er også en del av *National Strategy for Homeland Security*. Hensikten med strategien er å oppmuntre og bemyndige amerikanerne til å sikre de delene av cyberspace som de eier, opererer og kontrollerer. De strategiske målene for strategien er å forhindre cyberangrep mot kritiske infrastrukturer i USA, redusere nasjonal sårbarhet overfor cyberangrep, og begrense ødeleggelser fra cyberangrep som finner sted (Department of Homeland Security 2003:viii). "Cyber*terrorist* attacks" er ikke omtalt i dokumentet, kun "cyber attacks", og tiltakene som nevnes (fem nasjonale prioriteringer, som f.eks. planer om å etablere *National Cyberspace Security Response System* m.m) er bevis på sikkerhetiserende handlinger av The Department of Homeland Seucurity. Dette er for øvrig ikke tiltak som tidligere ville vært illegitime, prioriteringene er ikke knyttet til lovendringer, og er derfor ikke bevis på fullstendig sikkerhetisering av cyberterrorisme. Ett tiltak fra politisk hold i USA er også selve etableringen av Department of Homeland Security.

Alle etableringer av ulike sentre og departementer og knyttet til cyberangrep, cybertrusler, "cybercrime" m.m., er tiltak for å redusere disse truslene, men de er ikke ekstraordinære eller illegitime, så disse handlingene er sikkerhetiserende handlinger og ikke bevis på fullstendig sikkerhetisering. Nytolkning av lover eller nye lover som bryter med de prinsipper tidligere lovgivning bygger på kan derimot tolkes som sikkerhetiserende handlinger. Mye av terrorlovgivningen i USA og i EU som har kommet etter 11.september representerer brudd med det som tidligere ble sett på som sentrale rettigheter, og kan derfor tolkes som tegn på fullstendig sikkerhetisering. Anti-terrorlovgivningen som har blitt gjennomført i USA og Europa (særlig Storbritannia), har delvis krenket grunnleggende rettssikkerhetsprinsipper for

mistenkte terrorister og har legitimert brudd på menneskerettigheter gjennom kampen mot terror (Eide 2005). Terrorlovgivningen og datakriminalitetlovgivningen gjelder likevel terrorisme og datakriminalitet i sin helhet, og ikke cyberterrorisme spesifikt. Jeg vil derfor hevde at cyberterrorisme ikke har blitt *fullstendig* sikkerhetisert, men ja, sikkerhetisert gjennom en rekke tiltak rettet mot datakriminalitet og terrorisme. Terrorisme og datakriminalitet kan derimot sies å ha blitt fullstendig sikkerhetisert pga lovgivningen.

6.4.3 Konkluderende bemerkninger

Diskursanalysen viser at det finnes mange eksempler på sikkerhetiserende handlinger i forbindelse med den potensielle trusselen knyttet til cyberterrorisme, både fra akademikere og politikere. Talehandlingene er tegn på en prosess, en bevegelse, mot å gjøre cyberterrorisme til et sikkerhetsspørsmål på linje med andre trusler. ”Objektet” er ikke sikkerhetisert som sådan, i den forstand at jeg ikke har funnet bevis på at fullstendig sikkerhetisering har funnet sted, kun bevis på sikkerhetiserende handlinger (”securitizing moves”). Talehandlingene er ikke av en sånn art at de utpeker en eksistensiell trussel om krever umiddelbar handling, og hvor publikum aksepterer bruk av midler som fører til at de må frigjøre seg fra regler de ellers ville vært bundet av. Kildematerialet gir ikke grunnlag for å si at det er satt i gang konkrete tiltak rettet mot cyberterrorisme (ikke ekstraordinære/illegitime), kun tiltak i form av dokumenter som beskriver at cyberterrorisme og cybercrime må tas alvorlig. Jeg ser med andre ord en stor grad av sikkerhetisering og kan ikke snakke om en desikkerhetisering, til tross for at konklusjonen blir at ingen fullstendig sikkerhetisering av *cyberterrorisme* har funnet sted hittil.

I henhold til figur 1 (se 2.3) er cyberterrorisme analyseenheten og kritisk infrastruktur referanseobjektet. Diskursen bærer definitivt preg av at kritisk infrastruktur er definert som det som er eksistensielt truet av cyberterrorisme (og dens midler som datavirus, EMP-våpen m.m.) og/eller mindre lavskala-angrep, gjerne kalt cyberangrep. De fleste kildene viser til at utviklingen innen informasjons- og kommunikasjonssystemer og av

globale nettverk har ført til at de viktigste samfunnsfunksjonene våre er svært sårbare. I kjølvannet av denne erkjennelsen har bildet om en potensiell trussel fra cyberterrorister slått rot. Cyberspace er en ny arena for potensiell maktkamp. I denne arenaen er det ingen klart definerte grenser og det er vanskelig å håndheve lover. Denne utviklingen skaper nye problemstillinger for sikkerhetspolitikken. Har så cyberterrorisme blitt en del av den sikkerhetspolitiske agenda? Konklusjonen fra diskursanalysen er at vi har mange bevis på sikkerhetisering av cyberterrorisme, om enn ikke bevis på en fullstendig sikkerhetisering. Dette gjør likevel at jeg vil definere cyberterrorisme som en del av den sikkerhetspolitiske agenda. Akademikerne har bidratt sterkt til dette gjennom mange av sine sikkerhetiserende handlinger, men det er til syvende og sist politikerne som gjør saker til en del av sikkerhetspolitikken gjennom sine politiske (og sikkerhetiserende) handlinger. De politiske bidragene i diskursen viser at politikerne ikke har gjennomført særskilte tiltak direkte knyttet til begrepet cyberterrorisme, men tiltak relatert til trusselen fra ikke-statlige aktører som kan tenkes å utnytte teknologien i form av angrep mot kritisk infrastruktur, datakriminalitet m.m. Jeg vil hevde at cyberterrorisme har blitt en del av den sikkerhetspolitiske agenda, men fortsatt ikke i så stor grad som "tradisjonell" terrorisme har blitt det, ettersom det finnes lovgivning på anti-terrorbekjempelse og bekjempelse av datakriminalitet, men ikke lover rettet mot cyberterrorisme per se. En årsak til at cyberterrorismebegrepet ikke brukes innenfor enkelte politiske miljøer og at ingen tiltak er etablert direkte mot trusselen for cyberterrorisme, kan skyldes at vi ennå ikke har sett eksempler på rene cyberterroristangrep.

6.5 Oppsummering

Dette kapittelet har presentert de viktigste talehandlingene til de akademiske og sikkerhetiserende aktørene i forhold til en rekke momenter relatert til cyberterrorisme og lignende begreper. Diskursen har vist hva som regnes som trusler, hvorfor trusselen (for cyberterrorisme) finnes, konsekvenser av truslene m.m. Dette, samt analysen i kapittel 5, har gitt grunnlag for å kunne drøfte sikkerhetiseringsaspektet

ved cyberterrorisme og svare på den innledende problemstillingen. Gjennomgangen og presentasjonen av diskursen gir grunnlag for å konkludere med at det finnes mange eksempler på at det akademiske miljø bidrar i sikkerhetiseringsprosessen og sikkerhetiserer handlinger knyttet til cyberterrorisme. Diskursen i det politiske miljø, og tiltak gjennomført av politikere viser at de politiske sikkerhetiserende aktørene sikkerhetiserer cyberterrorisme, men en fullstendig sikkerhetisering av begrepet har ikke funnet sted på bakgrunn av mangel på kriterier som må oppfylles for å kunne definere en ”successful securitization”, jfr. kap.2.

7. Konklusjon og avsluttende betraktninger

”Cyberterrorisme – fakta eller fiksjon?” er denne oppgavens tittel. En oppgave om cyberterrorisme kunne vært skrevet på mange måter, og andre teorier og metoder enn de jeg har valgt kunne vært brukt, trolig også med relevante analyser og konklusjoner som resultat. Jeg synes imidlertid tilnærmingsmåten som har vært brukt i denne oppgaven har vært fruktbar og har gitt en interessant analyse av et nytt, og for mange fortsatt myteomspunnet, begrep. Det metodiske valget med å bruke diskursanalyse har vist seg svært nyttig for å få etablert en grundig presentasjon av hva cyberterrorisme er, hvem som ”snakker” om cyberterrorisme som en trussel, hvilke eksempler på cyberangrep som finnes, og hvilke tiltak som er satt i gang for å møte denne potensielle trusselen. Oppgaven har i tillegg et begrepsavklaringskapittel der ulike definisjoner av cyberterrorisme og beslektede begreper har blitt presentert, fordi det ikke finnes en allment brukt definisjon av cyberterrorisme. Valget av Københavnerskolen rammeverk som teorigrunnlag har også vært et godt valg ettersom det ved bruk av denne teorien har vært mulig å sette cyberterrorisme inn i en statsvitenskapelig sikkerhetskontekst. Talehandlingene i diskursen, satt inn i et teoretisk rammeverk, har gjort det mulig å svare på problemstillingen, og konklusjonen er at cyberterrorisme har blitt sikkerhetisert og er en del av den sikkerhetspolitiske agendaen, men det har ikke funnet sted en fullstendig sikkerhetisering.

I dette siste kapittelet vil jeg komme med noen betraktninger rundt ulike kildegrupper som er brukt i oppgaven siden kildene er svært sentrale i en diskursanalyse. Jeg vil spesielt se litt nærmere på mediekilder ettersom jeg valgte å utelate media som ”selvstendig” sikkerhetiserende aktør. Mange av de samme kildene går igjen når man søker etter informasjon og opplysninger om cyberterrorisme og beslektede begreper. Det kan være både på godt og vondt. Ved at det er få akademikere som forsker på dette feltet kan vi få god dybdeinformasjon siden de har valgt å satse på dette feltet og setter seg grundig inn i det. Det er en liten gruppe mennesker som samtidig får stor

makt og blir respektert siden de har et snevert fagområde. Samtidig vitner det kanskje om et lite miljø hvor rekrutteringen kan være et problem. Det kan igjen skyldes at forskningsfeltet er nytt, eller at det er få som anser cyberterrorisme mot kritisk infrastruktur som en aktuell sikkerhetstrussel og ikke har interesse av å studere det. Når det gjelder presseoppslag er det umulig å vite hva kildene har sagt konkret til artikkelforfatteren og om kildene blir korrekt gjengitt. Det er ikke grunn til å tro at opplysningene er feil, men det er en tilbakevendende problematikk med avis- og internettartikler. Det er alltid en mulighet for at intervju kan bli gjengitt med store mangler og at forskningslitteratur kan tolkes på en uriktig måte, og i tillegg kan informasjonen gå gjennom mange ledd før den kommer til artikkelforfatteren og noe informasjon kan dermed gå tapt. Media har gjerne sine egne standarder som preger seleksjonen og presentasjonen av informasjon.

Uttalelser fra høytstående personer og ledere kan ofte gjengis sensasjonelt i medier. Hovedessensen fra et foredrag eller intervju kan slås opp med en overskrift som fenger, men som av og til høres mer dramatisk ut enn det som er. Dessuten kan overskriften være misvisende for resten av artikkelens innhold. Avisartikler er basert på intervjuer og leste dokumenter og det er fra disse kildene ”den allmenne borger” skaffer seg det meste av informasjon. Det har stor betydning for folks oppfatninger om et tema hvordan stoffet blir gjengitt. Akademikere og offentlige tjenestemenn kan velge å uttale seg mer ”folkelig” for å få de fleste til å forstå hva de sier og i dette temaets tilfelle forstå at datatrussel mot infrastrukturer er alvorlig og et økende problem. De får en annen kontekst å uttrykke seg i, og man velger som regel forskjellige ord og uttrykksmåte til forskjellige sammenhenger. Som sagt så velger også media å omtale saker uten å ha foretatt intervju, men har brukt annen ”research”. Noen eksempler på dette følger nedenfor. BBC News (2000) har en artikkel som tar for seg avisers interesse for Love Bug-viruset. Her gjengis avisenes kommentarer til viruset og ordet ”cyberterrorisme” blir flere ganger nevnt. The Sun omtaler den filippinske hackeren som stod bak viruset en *cyberterrorist* og The Express frykter at *cyberterrorister* kan komme tilbake med en mer sofistikert versjon. Som nevnt flere

ganger i oppgaven finnes det ikke mange eksempler på terrorister som faktisk har benyttet seg av cybervåpen i noe som kan kalles et cyberterroristangrep. I alle kildene uttrykkes frykten for at dette skal skje, uten at man kan referere til noe som har skjedd. Pressen er på vakt overfor terroristers aktivitet og The Financial Times har en kommentar om den japanske kulten Aum Shinrikyo. Det viser seg at medlemmer av sekten har hatt tillatelse til å designe og installere sensitiv software i regjeringens datasystemer og slik kunne de hatt tilgang og mulighet til å samle informasjon om blant annet militære operasjoner (Tett & Nakamoto 2000). Regjeringsmedlemmer har sagt at sektmedlemmene ikke greide å skade nasjonale sikkerhetsinteresser og software de hadde installert er stoppet. Hendelsen har skapt bekymringer angående Japans kapasitet til å møte potensielle sikkerhetsproblemer innen informasjonsteknologi. I Indonesia advarte Timor-aktivister med Nobelprisvinner Jose Ramos Horta i spissen advart mot at hackere planla å sabotere Indonesias banksystem dersom de jukser i valget og motsetter seg Øst-Timors ønske om uavhengighet (BBC News 1999b). Konflikten mellom India og Pakistan blir utkjempet i cyberspace ettersom begge siden bruker elektronisk propaganda og sender ut støtende e-post (BBC News 1999).

Hvorfor blir cybertrusselen ansett som så *stor* spesielt innen akademia? Det gjør den også i media for den del, men der råder sensasjonslysten og krav om å selge i større grad vil jeg tro. Selv om det ikke er denne hovedoppgavens mål å finne årsaker til hvorfor trusselen blir ansett som så stor i akademia, er det et interessant spørsmål som jeg vil gi en kort kommentar.. Trusselvurderingene og scenariene som beskrives i mitt kildegrunnlag ser ikke ut til å ta høyde for framtidig utvikling på informasjons*sikring*. Vurderingene blir gjort på grunnlag av den teknologien vi hadde på tidspunktet vurderingene ble gjort og med den antakelsen at vi har de samme mulighetene om f.eks. 10 år. Det forutses at antallet cyberinntrengninger og angrep bare vil øke, noe som er sannsynlig dersom ikke motkrefter settes inn. Men økt antall angrep føre til større ønsker om å sikre seg mot disse angrepene, og teknologien vil trolig vil gjøre store framskritt på sikring av informasjonssystemene. Enkelte forskere har hevdet at

årsaken til de store trusselvurderingene ligger i et spørsmål om *penger*. Kan det være at forskningsinstitusjoner søker om større og større finansielle bevilgninger for å kunne fortsette og opprettholde driften av sin organisasjon? Er det slik at det legges fram forsterkede trusselscenarier for å sikre seg bevilgninger, selv om trusselen i realiteten ikke er så stor som de hevder? Disse spørsmålene får stå ubesvart, men det skal ikke underslås at de fleste forskere nok har en genuin *interesse* for forskningen de utfører og er ikke drevet av penger.

Når det gjelder de politiske kildene, stedet hvor vi finner de reelle mulighetene til bevis på fullstendig sikkerhetisering, har vi sett at politikerne oppfatter kritisk infrastruktur (som referanseobjekt) som truet på grunn av globalisering og avhengighet av informasjonsteknologi. Både media og akademikere, i tillegg til politikere, er med på å fremheve infrastruktur som en livsviktig funksjon som kan lamme samfunnet ved ødeleggelse, derfor må denne beskyttes. Alle disse aktørenes utsagn (både trusselvurderinger, definisjoner og eksempler) er sikkerhetiserende handlinger, men politikerne har mulighet til å gjennomføre en fullstendig sikkerhetisering av cyberterrorisme. Kildene viser at begrepet cyberterrorisme fortsatt er mer fremtredende i akademia og media enn i politikken. I det politiske liv er man absolutt opptatt av farene knyttet til ondsinnede handlinger rettet mot samfunnets kritiske infrastrukturer, men tiltakene de setter i gang har ”tradisjonell” terrorisme og ”cybercrime” som fokus. Man kan kanskje si at det er cyberterrorismens *potensiale* som skaper rom for at trusselen blir gjort til et sikkerhetsanliggende. Som sagt flere ganger gjennom oppgaven, er det ingen eksempler så langt på cyberterroristangrep, men forskningen viser at potensialet er til stede. Politikerne tar denne trusselen på alvor gjennom økte sikringstiltak i kritiske samfunnssektorer, men det finnes ikke uttalte politiske ytringer hvor begrepet cyberterrorisme i seg selv blir ansett som en trussel. Utsagn som viser en frykt for at ikke-statlige grupperinger kan ta i bruk moderne teknologiske midler og våpen og rette angrep via globale nettverk med mål å ramme kritiske infrastrukturer er likevel tilstede. Disse er bevis på en frykt for cyberterrorisme selv om den ikke er uttalt bokstavelig. Sikkerhetsdiskursen har vært preget av en rekke problemstillinger og dilemmaer i forhold til framveksten av

cyberterrorisme som trussel. På den ene siden har diskursen vært preget av frykten for et "elektronisk Pearl Harbor" med cyberkrig og informasjonskrigføring. På den andre siden har man vært opptatt av problematikk rundt eierskap av kritisk infrastruktur (offentlig vs. privat) og gjensidig avhengighet av vitale samfunnsfunksjoner. Offentlig og privat sektor, i alle fall i USA hvor det for øvrig har vært stor splid rundt dette, kan bruke ulike kriterier for å definere risiko og sårbarhet, og de kan ha ulike oppfatning av sikringsnivå og hva man ønsker å sikre. Private eiere kan være mer opptatt av å hindre systeminntrengning i sin virksomhets informasjonssystemer enn å tenke på nasjonal sikkerhet som sådan.

Avslutningsvis vil jeg spørre, hva har skjedd etter 2003? I denne oppgaven ville jeg først fokusere på årene fram og til og med 2000-års skiftet (år da man så en eksplosiv utvikling av datateknologi og nettbruk), men ettersom 11.september-angrepene i 2001 viste seg å bli så fundamentalt viktige for vår oppfatning av trussel- og risikobildet de senere år, utvidet jeg rammen for oppgaven til 2003. Det har kommet ut mange politiske dokumenter etter dette, lovverket innen bekjempelse av terrorisme har endret seg kraftig, og forskere har fortsatt å utgi artikler og bøker om cybertrusselen. Vi er fortsatt like globaliserte og avhengige av Internett, så trusselen for cyberangrep, og om mulig cyberterrortrusselen, er absolutt til stede. Men det hele bunner i en *potensiell* trussel eller fare. Det er kanskje derfor en raskt søk og overblikk etter kilder fra 2003 og fram til i dag viser at det ikke har skjedd noe radikalt innen temaet cyberterrorisme. Begrepet er ikke sentralt i viktige dokumenter, det domineres av datakriminalitet og terrorisme, og selvsagt kan årsaken være at det ennå ikke har funnet sted et cyberterroristangrep som har elementer har terror i seg. Kan det være et stort angrep må finne sted før vi ser endring i lovgivning og andre tiltak på dette området? Vi så en stor endring i fokus på terrorisme etter det spektakulære angrepet på tvillingtårnene i New York, og det har ført til endringer i lover og har også hatt betydning for folk, jf, strengere sikkerhetskrav ved flyving. Angrepene i Madrid i 2004 og London i 2005 var også bevis på hvor sårbare vi er. Selv om dette ikke var cyber-relaterte angrep så har de skapt en økt frykt for terrorisme generelt i særlig

vestlige samfunn, og media har også gitt oss en bevissthet og kunnskap om at terrororganisasjoner som al-Qaida bruker Internett aktivt til propaganda, informasjonsinnhenting, anerkjennelse for gjennomførte operasjoner, pengeinnsamling m.m. Dette bidrar til å skape en kontinuerlig frykt for at ondsinnede aktører kan gjennomføre ondsinnede handlinger mot våre sårbare systemer ved hjelp av ny teknologi. Kanskje må vi se et reelt cyberterroristangrep før politikerne setter i gang ekstraordinære tiltak for å møte trusselen for *cyberterrorisme*. Foreløpig er cyberterrorisme en potensiell trussel som er gjort til et sikkerhetsanliggende på den sikkerhetspolitiske agenda, men ikke sikkerhetisert fullt ut.

8. Litteraturliste

Aftenposten (2004): "Myndigheter advarer mot dataterror", 2.august [online].

Alexander, Yonah & Michael S. Swetnam (red.) (2001): *Cyber terrorism and information warfare: threats and responses*. Ardsley, N.Y.: Transnational Publishers.

Arquilla, John & David Ronfeldt (1993): "Cyberwar is coming!" Tilgjengelig via http://gopher.well.sf.ca.us:70/0/Military/cyberwar. Finnes også som kap. 2 i John Arquilla & David Ronfeldt (red.)(1997): *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, California: RAND.

Arquilla, John & David Ronfeldt & Michele Zanini (1998): "Networks, Netwar, and Information- Age Terrorism", kap. 3 i Ian Lesser m.fl. (1998): *Countering the New Terrorism*. Santa Monica & Washington D.C.: RAND.

Arquilla, John & David Ronfeldt & Michele Zanini (1999): "Networks, Netwar, and Information-Age Terrorism", kap. 4 i Zalmay Khalilzad, John P. White & Andrew W. Marshall (red.): *The Changing Role of Information in Warfare*. Santa Monica: RAND.

Arquilla, John (1999b):"Ethics and Information Warfare", kap 13. i Khalilzad, Zalmay, John P. White & Andrew W. Marshall (red.): *The Changing Role of Information in Warfare*. Santa Monica: RAND.

Baldwin, David A. (1997): "The concept of security", *Review of International Studies*, 23: 5-26.

BBC News (1999): "Kashmir's cyberwar", 28. juni [online].

BBC News (1999b): "Timor activists warn of cyber war", 18. august [online].

BBC News (2000): "Papers fall for Love Bug", 5. mai [online].

BBC News (2000): "Cyber-terrorists wield weapons of mass disruption", 22. februar [online].

BBC News (2001): "Straw defends new terrorism", 19. februar [online].

BBC News (2003): “Cyber terrorism ‘overhyped’”, 14.mars [online].

Bequai, August (1987): *Technocrimes*. Lexington, Mass. : Lexington Books.

Borland, John (1998, September 23). Analyzing The Threat Of Cyberterrorism I. TechWeb [online]. Tilgjengelig via www.techweb.com

Bunker, Robert J. (1999): “Higher-dimensional warfighting”, *Military Review*, Sep/Oct, Vol.79, No.5.

Buzan, Barry (1991): *People, states & fear; an agenda for internastional security studies in the post-cold war era*. Hemel Hempstead: Harvester Wheatsheaf.

Buzan, Barry (1993):”Introduction: The changing security agenda in Europe”, kap. 1 i Ole Wæver, Barry Buzan, Morten Kelstrup & Pierre Lemaitre (1993): *Identity, Migration and the New Security Agenda in Europe*. New York: St. Martin’s Press.

Buzan, Barry (1995): “Security, the State, the “New World Order”, and Beyond”, kap. 7 i Ronnie D. Lipschutz (red.): *On Security*. New York: Columbia University Press.

Buzan, Barry (1997):”Rethinking Security after the Cold War”, *Cooperation and Conflict*, 32 (1): 5-28.

Buzan, Barry, Ole Waæver & Jaap de Wilde (1998): *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers.

Castells, Manuel (1999): ”Information technology, globalization and social development”, UNRISD (United Nations Research Institute for Social Development), Discussion Paper 114, September.

Center for Strategic and International Studies, CSIS (1998):“Cybercrime… Cyberterrorism…Cyberwarfare…: Averting an Electronic Waterloo”. CSIS Task Force Report. Washington D.C.: CSIS.

CNN Norge (2000): ”USA frykter Pearl Harbor i cyberspace”, 9. desember [online].

Collin, Barry C. (1997, mars). The Future of Cyberterrorism I: Crime and Justice International [online]. -Vol.13, no.2. - Tilgjengelig via: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=415

Congressional Bill (2001):"Cyber Security Information Act – H.R.2435", 10.juli.

Denning, Dorothy E. (1999): *Information Warfare and Security*. Reading, Massachusets: ACM Press.

Denning, Dorothy E. (2000):"Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", Georgetown University. Tilgjengelig via: http://www.iwar.org.uk/cyberterror/resources/denning.html

Denning, Dorothy E. (2000b): "Cyberterrorism". Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives. 23. mai. Tilgjengelig via: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Dennis, Ian (1998): "Globalization Process and Acquisitions of New Technology", kap. 7 i Gunnar Jervas (red.): *FOA Report on Terrorism*. Stockholm: FOA.

Department of Homeland Security (2003):"The National Strategy to Secure Cyberspace", Februar. Tilgjengelig via: http://www.dhs.gov/xlibrary/assets/ National_ Cyberspace_ Strategy. pdf

Det amerikanske justisdepartementet (1998): "Attorney General Reno unveils new Critical Infrastructure Protection Center". Pressemelding, 27. februar.

Devost, Matthew G. (1995): "National Security in the Information Age". MA Thesis in Political Science, University of Vermont, USA. Tilgjengelig via: http://www.terrorism.com/documents/devostthesis.html

Easton, Mark (2000, Mars 23): Fighting Cybercrime I: Channel 4 News [online].

Eide, Petter (2005):"Endring i sikte?" Uttalelse fra generalsekretæren i Amnesty International Norge. 14. desember. Tilgjengelig via: http://www.amnesty.no/web.nsf/pages/B92FDDE160E570C0C12570CF004BFE11

Engene, Jan Oskar (1994): *Europeisk terrorisme. Vold stat og legitimitet*. Oslo: TANO.

Eriksson, E. Anders (1999): “Information Warfare: Hype or Reality?”, *The Nonproliferation Review* 6:3 Spring-Summer.

EU-kommisjonen (2000):”Et sikrere informationssamfund: Højnelse af sikkerheden i informationsinfrastrukturerne og bekæmpelse af computerrelateret kriminalitet”. Meddelelse fra kommisjonen til rådet, Europa-parlamentet, det økonomiske og sociale udvalg og regionsudvalget. KOMM (2000) 890.

EU-kommisjonen (2001):”Net- og informationssikkerhed: Forslag til en europæisk strategi”. Meddelelse fra kommisjonen til rådet, Europa-parlamentet, det økonomiske og sociale udvalg og regionsudvalget. KOMM (2001) 298.

Flynt, Bill (2000): “Threat Kingdom”, *Military Review*, July-August.

Forsvarets fellesoperative doktrine (2000): Del B – Operasjoner. Oslo: Forsvarets overkommando, februar.

Furnell, S.M & M.J. Warren (1999): “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millenium?”, *Computers & Security* 18: 28-34.

Grunnan, Tonje (2000): “Deltakelse på konferansen Information Warfare Post Y2K: A National Security Perspective i Washington D.C., 11.-12. mai 2000. FFI/Reiserapport - 2000/03881. Kjeller: Forsvarets Forskningsinstitutt.

Gude, Benedicte (1998): “Informasjonsoperasjoner – utfordringer for hele samfunnet”. Foredrag for FO/E, 28. oktober.

Heggelund, Trond (1999, September 2): POT bygger enhet mot kyberterror I. Computerworld [online].

Hellevik, Ottar (1991): *Forskningsmetode i sosiologi og statsvitenskap*. Oslo: Universitetsforlaget.

Hirst, Peter F. (1998): ”New and Old Technologies: Choice of Strategy and Targets”, kap. 6 i Gunnar Jervas (red.): *FOA Report on Terrorism*. Stockholm: FOA.

Hoffman, Bruce (1998): *Inside Terrorism*. New York: Columbia University Press.

Hoffman, Bruce (2000): "Workshop med TERRA-prosjektet ved Forsvarets forskningsinstitutt", 26. september.

IT-avisen (2000): "Neste krig kommer på nett". 17. oktober [online].

James, Leah & Jestyn Cooper (2000): "Organised exploitation of the information super-highway", *Jane's Intelligence Review*. July.

Johansen, Iver (2004): "Cyberspace som slagmark: Refleksjoner omkring Internett som arena for terrorangrep". Kjeller: FFI/Rapport-2004/01666.

Jørgensen, Marianne Winther & Louise Phillips (1999): *Diskursanalyse som teori og metode*. Fredriksberg: Roskilde Universitetsforlag.

Khalilzad, Zalmay (1999): "Defense in a Wired World: Protection, Deterrence, and Prevention", kap. 14 i Khalilzad, Zalmay, John P. White & Andrew W. Marshall (red.): *The Changing Role of Information in Warfare*. Santa Monica: RAND.

Krutskikh, A. (1999): "Information Challenges to Security", *International Affairs* 45 (2): 29-36.

Lee, Sungkoo (1999): "Constructing International Cooperative Organizations for Defending Information Terrorism". Presentert på konferansen Developments in the Field of Information and Telecommunications in the Context of International Security. Genève, 25.-26. august. Konferansepaper.

Lia, Brynjar (2000): " Er sivil infrastruktur sannsynlege mål for terrorgrupper i fredstid? Nokre førebelse konklusjonar om terrorisme som tryggjingspolitisk utfordring i Norge". Kjeller: FFI/Rapport-2000/01703.

Lia, Brynjar & Annika S. Hansen (2000): "Globalisation and the Future of Terrorism: Patterns and Predictions". Kjeller: FFI/Rapport – 2000/01704.

Lia, Brynjar & Rolf-Inge Vogt Andrésen (2000): "Terrorism, political violence and organised crime – security policy challenges of non-state actors' use of violence. Proceedings from an International Seminar in Oslo". Kjeller: FFI/Rapport – 2000/06444.

Lia, Brynjar (2007): ”Jihadi Web Media Production: Charatcertistics, trends, and future implications”. Presentert på ”Check the Web” Conference on “Monitoring, Research and Analysis of Jihadist Activities on the Internet – Ways to deal with the issue”, Berlin 26.-27. februar. Konferansepaper.

Libicki, Martin C. (1995): *What is Information Warfare?* Washington DC: NDU Press.

Lipschutz, Ronnie D. (1995): ”On Security”, kap.1 i Ronnie D. Lipschutz (red.): *On Security*. New York: Columbia University Press.

Mathisen, Werner Christie (1997): ”Diskursanalyse for statsvitere: Hva, hvorfor og hvordan”. Institutt for statsvitenskap, Det samfunnsvitenskapelige fakultet, Universitet i Oslo. Forskningsnotat 1/1997.

MC 422, *NATO Information Operations* (1998). Brussel: North Atlantic Military Committee.

McSweeney, Bill (1996): Identity and security: Buzan and the Copenhagen school”, *Review of International Studies* 22: 81-93.

Molander, Roger C., Andrew S. Riddle & Peter A. Wilson (1996): *Strategic Information Warfare – A New Face of War*. Santa Monica: RAND.

NATO, Research and Technology Organisation (2006): ”Information Operations – Analysis Support and Capability Requirements”, RTO Technical Report, TR-SAS-057, Oktober.

Nettavisen (2005): ”Norge dårlig sikret: -Frykter cyberterror fra al-Qaida”, 16.april [online].

Neumann, Iver B. (2001): *Mening, materialitet, makt: En innføring i diskursanalyse*. Bergen: Fagbokforlaget.

NOU (2000: 24): *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapssamarbeidet i samfunnet.* Oslo: Statens forvaltningstjeneste, Informasjonsforvaltning.

Nærings- og handelsdepartementet (2000): ”Samfunnets sårbarhet som følge av avhengighet til IT”. Rapport. Oktober. Oslo.

O’Day, Alan (red.)(2004): *Cyberterrorism.* Aldershot:Ashgate.

O'Brien, Kevin (2000): "Information Operations and Operation "Allied Force"". Presentert på konferansen Information Warfare Post Y2K: A National Security Perspective. Washington D.C., 11.-12. mai. Konferansepaper.

O'Brien, Kevin & Joseph Nusbaum (2000): "Intelligence collection for asymmetric threat – part two", *Jane's Intelligence Review*, November.

Pollitt, Mark M.: "Cyberterrorism – Fact or Fancy?". Paper. George Washington University. Tilgjengelig via: http://www.cs.georgetown.edu/-denning/infosec/pollitt.html

Potmoac Proceedings Report (1998): "Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses", Proceedings Report, PIPS-98-2, 16. april. Arlington, Virginia: Potomac Institute for Policy Studies.

Rathmell, Andrew (1997, oktober): Cyber-terrorism: The Shape of Future Conflict? -s.40-46 I: Royal United Service Institute Journal [online]. Tilgjengelig via: http://www.kcl.ac.uk/orgs/icsa/Old/rusi.html

Rathmell, Andrew, Richard Overill, Lorenzo Valeri & John Gearson (1997): "The IW Threat from Sub-State Groups: an Interdisciplinary Approach". Presentert på The Third International Symposium on Command and Control Research and Technology, Institute for National Strategic Studies, National Defense University. June 17-20. Konferansepaper.

Regan, Tom (1999, July 1). How terrorists use the Internet to spread their messages I. The Christian Science Monitor [online]. Tilgjengelig via: http://www.csmonitor.com/durable/1999/07/01/messages.html

Reno, Janet (1998): *Address by Attorney general Janet Reno*. Conference on Critical Infrastructure Protection. Lawrence Livermore National Laboratory, Livermore, California. 27. februar.

Rodal, Siv Kjersti (2000): "Deltagelse på konferansen "Cyberterrorism: The Risks and Realities" i Washington D.C. og besøk ved Institute for Defense Analysis (IDA) i Alexandria, Virginia, 16-17 November 1999". Kjeller: FFI/Reiserapport – 2000/00074.

Rodal, Siv Kjersti (2001): *Personlige samtaler med forskeren*, våren.

Ronfeldt, David & Armando Martínez (1997): "A Comment on the Zapatista Netwar", kap. 16 i Arquilla, John & David Ronfeldt (red.): *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND.

Shapiro, Jeremy (1999): "Information and war: Is it a revolution?", kap. 5 i Zalmay M. Khalilzad & John P. White (red.): *The Changing Role of Information in Warfare*. Santa Monica: RAND.

Stalsberg, Tom (2000, August 28). Livsfarlige hackere I:Dagbladet [online]

Stark, Rod (1999):"Cyber Terrorism: Rethinking New Technology". Department of Defense & Strategic Studies, Southwest Missouri State University. Tilgjengelig via: http://www.infowar.com/mil_c4i/stark/Cyber_terrorism_Rethinking_New_Technology1.html

Stewart, Bernard L.(1987): "Information and Communications: An Introduction", *Terrorism* 10 (3): 251- 274.

Stortingsmelding nr. 17 (2001-2002): *Samfunnssikkerhet*. Justis- og politidepartementet, Oslo.

Stortingsmelding nr. 22 (1997-98): *Hovedretningslinjer for Forsvarets virksomhet og utvikling i tiden 1999-2002*. Forsvarsdepartementet, Oslo.

Tett, Gillian & Michiyo Nakamoto (2000, mars 2): Aum cult installed software in Japanese government systems I: Financial Times [online].

The Council of Europe and Cybercrime: "Cybercrime – the facts/The council of Europe Cybercrime Convention". Faktaark. Tilgjengelig via: www.coe.int/cybercrime

The Council of Europe (2001): "Convention on Cybercrime". Treaty no. 185. Budapest, 23. november. Tilgjengelig via: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Toffler, Alvin & Heidi Toffler (1993): *War and Anti-War: survival at the dawn of the 21st century*. London: Little Brown and Company.

Tsygichko, Vitali N. (1999): ”Modern Information Technologies and Information Security”. Presentert på konferansen Developments in the Field of Information and Telecommunications in the Context of International Security. Genève, 25.-26. august. Konferansepaper.

USA Today (1998): “Lawmakers: Cyber terrorism is a worry”. 11. juni [online].

Vatis, Michael A. (1998): “New NIPC Seeks Govt., Industry Alliance”, *National Security Institute’s*, ADVISORY, Juli 1998.

VG-Nett (2001): “Norge uten forsvar mot nett-terrorisme”, 3.august [online].

Viken, Tonje Merete (1999, August 9). Kina drømmer om krig uten grenser I: Dagbladet [online].

Votrin, Dmitry S. (1999): ”On the future of the international information security regime”. Presentert på konferansen Developments in the Field of Information and Telecommunications in the Context of International Security. Genève, 25.-26. august. Konferansepaper.

Whine, Michael (1999): ”Islamist Organisations on the Internet”, *Terrorism and Political Violence* 11 (1): 123-132.

White Paper (1998): “The Clinton Administration’s Policy on Critical Infrastrucure Protection: Presidential Decision Directive 63”, 22. mai.

Wæver, Ole (1995): ”Securitization and Desecuritization”, kap.3 i Ronnie D. Lipschutz (red.): *On Security*. New York: Columbia University Press.

Yin, Robert K. (1994): *Case Study Research, Design and Methods*, 2.utgave. Thousand Oaks: SAGE Publications.

Østerud, Øyvind & Kjell Goldmann & Mogens N. Pedersen (red.)(1997). *Statvitenskapelig leksikon*. Oslo: Universitetsforlaget.

Østerud, Øyvind (1999): *Globaliseringen og nasjonalstaten*. Oslo: Ad Notam Gyldendal.